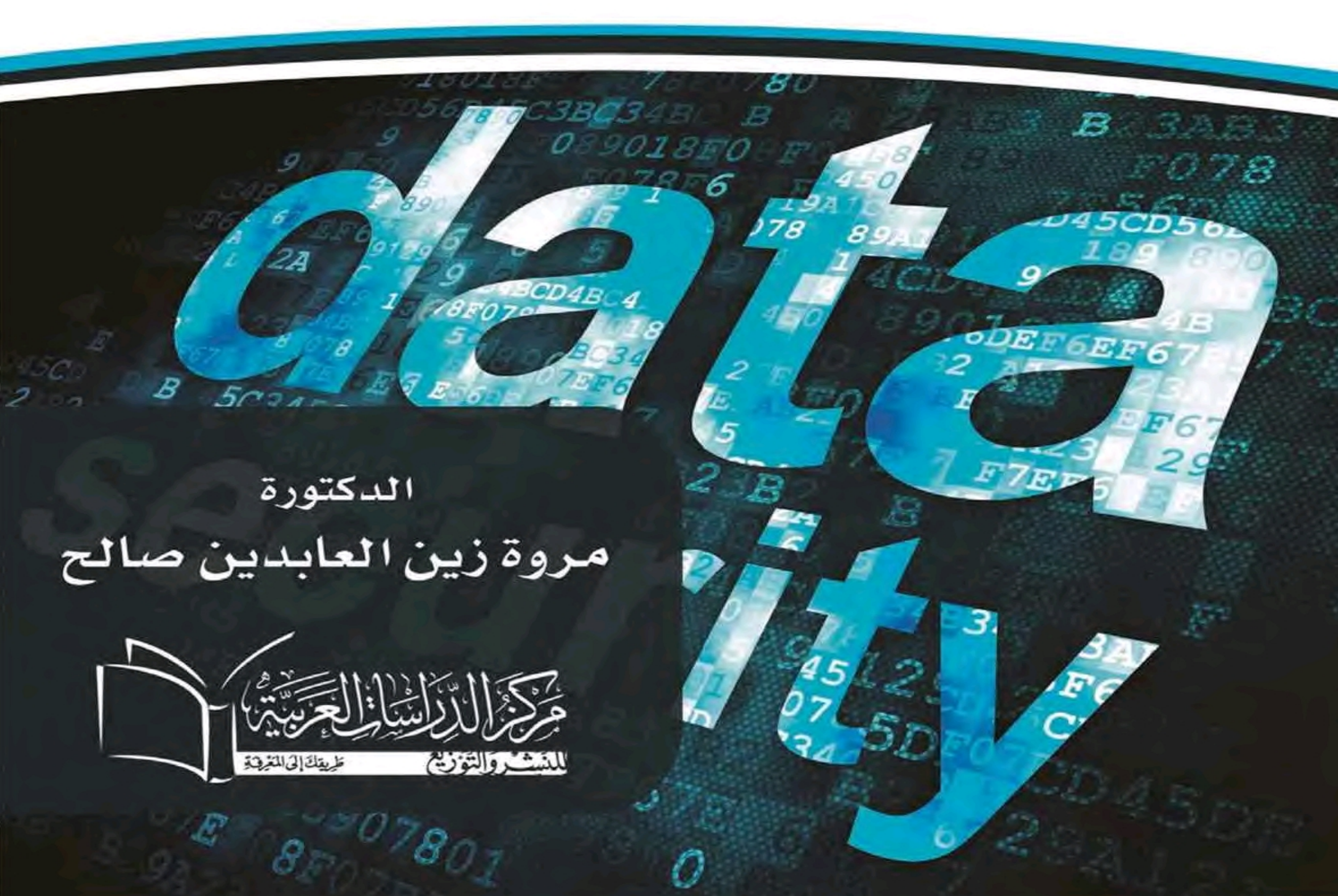
الحماية القانونية الدولية للبيانات الشخصية عبر الإنترنت

بين القانون الدولي الاتفاقي والقانون الوطني



الدكتورة

مروة زين العابدين صالح

مركز الدراسات العربية للنشر والتوزيع

طريقك إلى المعرفة

الحماية القانونية الدولية للبيانات الشخصية عبر الإنترنت



الحماية القانونية الدولية

للبيانات الشخصية عبر الإنترنت

بين القانون الدولي الاتفاقي والقانون الوطني

الدكتورة

مروة زين العابدين صالح

الطبعة الأولى

1437هـ- 2016 م



رقم الإيداع

2015/5118

ISBN 978-977-6504-91-2



مركز الدراسات العربية للنشر والتوزيع

طريقك إلى المعرفة

جمهورية مصر العربية

الجيزة - 6 أكتوبر - الحي الخامس - ش 13

002 (02) 383 767 64

002 0100440 490 6

002 0101127 0909

00966 543 044 662

www.ascpublishing.com

info@ascpublishing.com

ahmed.tafesh@gmail.com

بسم الله الرحمن الرحيم

﴿قُل رَّبِّ أَدْخِلْنِي مُدْخَلَ صِدْقٍ وَأَخْرِجْنِي مُخْرَجَ صِدْقٍ وَاجْعَل لِّي مِن لَّدُنكَ سُلْطَانًا نَّصِيرًا﴾

إهداء

إلى ابنتـي .... قرة عيني

وأبي العزيز

وأمي الغالية

وزوجي الحبيب

وأصدقائي الأعزاء

وكل من سـاعدني لأتم هذا البحث

الباحثة

شكر وتقدير

الحمد لله الذي لا يبلغ مدحته القائلون.

الحمد لله رب العالمين الذي علم بالقلم، علم الإنسان ما لم يعلم.

ووتد بالصخور ميدان أرضه. أحمده استتماماً لنعمته. واستسلاماً لعزته. واستعصاماً من معصيته. وأستعينه فاقة إلى كفايته. أنه لا يضل من هداه.

وأشهد أن لا إله إلا الله وحده لا شريك له. شهادة ممتحناً أخلاصها. نتمسك بها أبداً ما أبقانا.

وأشهد أن محمداً عبد الله ورسوله. أرسله بالدين المشهور. والعلم المأثور. والكتاب المسطور. والنور الساطع. والضياء اللامع.

أما بعد:

فإنني لا أملك إلا أن أبوح بكلمة شكر لمن يستحق الشكر بعد الله عزّ وجلّ.

يقول النبي المعصوم ﷺ "لا يشكر الله من لا يشكر الناس"... ويقول "ومن صنع إليكم معروفاً فكافئوه فإن لم تجدوا ما تكافئونه فاذعوا له حتى تروا أنكم قد كافأتموه".

ومـن هنـا لا يسـعني في هـذا المقـام إلا أن أتقـدم بخالـص آيـات التقديـر الجليـل والشـكر الوفـير المقرونـين بالاحـترام والامتنـان لأسـتاذي القديـر الأسـتاذ الدكتـور/ عصـام الديـن القصبـي – أسـتاذ القانـون الـدولي الخـاص - بحقـوق عـين شـمس، عـلى تفضلـه وبرغـم كـثرة مشـاغله بقبـول الاشـتراك في الإشراف عـلى رسـالتي هـذه. فشـملني بعلمـه الغزيـر وخلقـه الرفيـع وفضلـه الوفـير وهمتـه العاليـة، وجـزاه اللـه عنـي خـير الجـزاء، ونفـع اللـه بعلمـه رواد العلـم والمعرفـة، وأدام اللـه في عمـره، ومتعـه بالصحـة والعافية.

وانطلاقـاً مـن هـذا التوجيـه النبـوي، واعترافـاً بالفضـل والجميـل، فإنه لا يسـعني في هـذا المقـام إلا أن أتقـدم بخالـص الشـكر والتقديـر وعظيـم العرفـان والامتنـان إلى أسـتاذي الفاضـل العـالم الفقيـه الدكتـور/ أبـو العـلا عـلي أبو العـلا النمر - أسـتاذ ورئيس قسـم القانـون الـدولي الخـاص - بكليـة الحقـوق بجامعة عين شـمس، على تفضلـه بقبول الإشراف عـلى هـذه الرسـالة، والـذي تعهـدني برعايتـه وشـملني بعطفـه، ولم يضـن عـلى بعلمـه الغزيـر، ولم يضـق ذرعـاً بي رغـم أعبائـه الكثـيرة ومشـاغله الجمـة، فآثـرني برحابة صـدره وتواضعـه وفيـض عطائـه، ومزيـد كرمه، ولقـد كانـت توجيهاتـه القيمـة ونصائحه الثمينـة بمثابـة النـبراس الـذي ينـير عتمـة دروب البحـث الوعـرة، فـكان العقـل المنير الـذي عـبر معـي ظـلام الحـيرة فأضـاء بحثـي حتـى وصلنـا معـا إلى شـاطئ النـور، فجـزاه اللـه عنـي وعـن طـلاب العلـم خـير الجـزاء، ومتعـه بموفـور الصحـة والعافية.

وكذلـك أتوجـه بخالـص شـكري وتقديـري، وعظيـم عرفـاني وأمتنـاني إلى أسـتاذى الفاضـل العـالم الجليـل الأسـتاذ الدكتـور/ أحمـد قسـمت الجـداوي - أسـتاذ القانـون الـدولي الخـاص - بكليـة الحقـوق جامعـة عـين شـمس، عـلى قبولـه رئاسـة لجنـة الحكـم عـلى هـذه الرسـالة، وتحملـه عنـاء قراءتهـا، رغـم مشـاغله وأعبائـه الكثـيرة، فلسـيادته منـي كل الشـكر والامتنـان، وجـزاه اللـه عنـي خـير الجـزاء، ونفـع اللـه بعلمـه رواد العلم والمعرفـة، وأدام اللـه في عمـره، ومتعـه بالصحـة والعافيـة.

كما أتقدم أيضاً، بخالص شكري وعظيم امتناني وتقديري للأستاذ الدكتور/ جمال الكردي أستاذ القانون الدولي الخاص - بكلية الحقوق جامعة طنطا، لتحمله عناء قراءة هذه الرسالة، والاشتراك في لجنة الحكم عليها، رغم ضيق وقته ومشاغله الكثيرة، فلسيادته مني كل الشكر والتقدير والامتنان، وجزاه الله تعالى عني خير الجزاء، ومتعه بموفور الصحة والعافية.

"أسأل الله تعالى أن يجزيهم خير الثواب"

الباحثة

مقدمة

أولاً: أهمية الموضوع:

مع التطور التكنولوجي الهائل، والعالم المنفتح الذي أصبحنا نعيش فيه تغير مفهوم الخصوصية المادية وتحور إلى أن شمل البيانات الشخصية إذ أنه مع زيادة استخدام التكنولوجيا وتطور تقنيات التواصل، والزيادة المطردة في استخدام الإنترنت ووسائل التواصل المتطورة، نشأ خطر يهدد البيانات الشخصية للأفراد من حيث الحصول عليها وتداولها ومعالجتها، وكذلك اختلفت صور الاستيلاء عليها، وبالتطور التكنولوجي أيضا تطورت طرق إساءة استغلال تلك البيانات، وعلى ذلك وجب دراسة مثل هذا الموضوع لأهميته البالغة وذلك بالاقتران مع ما قد لوحظ من إهمال البيئة التشريعية العربية لمثل هذه التشريعات مقارنة بالتشريعات في الدول الأخرى، والتي على الرغم من محاولتها فرض حماية قانونية على البيانات الشخصية عبر الإنترنت فإن مثل هذه الحماية لم توفر الأمان الكامل للبيانات الشخصية المتداولة عبر الإنترنت.

وإضافة إلى أن المجتمع الرقمي يتطلب وجود نوع من التفاعل الآمن والفوري بين خدمات إلكترونية عالية المستوى والفاعلية تقدم من قبل مؤسسات حكومية أو خاصة وبين أفراد من المجتمع للاستفادة من تلك

الخدمات. وهذا لن يتأتى إلا لو أحس الأفراد بالأمن والثقة، ومن هنا تأتي أهمية هذا البحث في كونه محاولة متواضعة من الباحث لتسليط الضوء على الخصوصية المعلوماتية وأهميتها، ومخاطر التقنيات الحديثة عليها، وكيفية الحماية التي وفرها مشروع قانون المعاملات الإلكترونية لها.

و من ثم تم فرض صور من الحماية على تلك البيانات في مختلف التشريعات، ولكن واجهت حماية البيانات الشخصية في البيئة العربية قصورا هائلاً، حيث مازالت حماية البيانات الشخصية تناقش في ظل القواعد العامة، وليست هناك ثمة قوانين واضحة محددة تنظمها.

ثانياً: تحديد الموضوع:

سيتم التطرق من خلال هذه الدراسة إلى مفهوم خصوصية البيانات، وكيفية معالجته في التشريعات العربية والمقارنة، وكذلك كيفية حماية البيانات الشخصية في ظل التطور التكنولوجي الهائل وثورة الاتصالات والإنترنت، إضافة إلى صور من الجرائم الإلكترونية التي تهدد البيانات الشخصية إثر تداولها عبر الإنترنت.

ثالثاً: منهج البحث:

يعتمد البحث على المنهج التحليلي المقارن في دراسة نصوص القواعد القانونية ذات الصلة بموضوع البحث الواردة في التشريعات الدولية والاتفاقيات والتوجيهات والمقارنة بينها، ومحاولة تحليلها لبيان مدى إسهام كل منها في إيجاد الحلول المناسبة لما يثيره موضوع البحث من إشكاليات لدى إعماله عليها.

كما يعتمد في بعض مواضيعه على المنهج التاريخي وذلك في بيان نشأة وتطور القواعد التي تحكم الخصوصية، وخاصة خصوصية البيانات الشخصية في ظل العصر التكنولوجي والرقمي للوقوف على جذور نشأتها الأصلية، والظروف التي أدت إلى تطورها باختلاف مرجعياتها، والمحل

المنوط بالحماية من تلك البيانات وذلك للوصول إلى أصل قانوني لحماية البيانات الشخصية والتي يتم تداولها عبر الإنترنت.

رابعاً: أهداف البحث:

1 - تسليط الضوء على الحق في الخصوصية المعلوماتية.

2 - الكشف عن مخاطر التقنيات الحديثة على الحق في الخصوصية المعلوماتية.

3 - إيضاح جهود التشريعات المختلفة في حقل حماية البيانات الشخصية في بيئة الإنترنت.

خامساً: تقسيم الموضوع:

ينقسم البحث بابين رئيسين:

الباب الأول: مفهوم البيانات الشخصية، وإطار حمايتها في التشريعات المختلفة.

الفصل الأول: ماهية البيانات الشخصية.

الفصل الثاني: الحماية القانونية للبيانات الشخصية.

الباب الثاني: حماية البيانات الشخصية المتداولة عبر الإنترنت.

الفصل الأول: المخاطر التي تهدد خصوصية البيانات عبر شبكة الإنترنت.

الفصل الثاني: الحماية الجنائية للبيانات الشخصية عبر شبكة الإنترنت.

الباب الأول

مفهوم البيانات الشخصية و إطار حمايتها في التشريعات المختلفة

تمهيد وتقسيم:

عند تناول حماية البيانات الشخصية بالدراسة وجب بداية توضيح:

- ماهية البيانات الشخصية من حيث التعريف ونشأة فكرة خصوصية البيانات والتي انبثقت من المفهوم العام للخصوصية **(الفصل الأول)**.
- وكذلك تعين على الباحث دراسة مجموعة من القوانين التي فرضت حماية للبيانات الشخصية، والمبادئ الأساسية لتلك الحماية مع توضيح موقف المشرع العربي من حماية البيانات الشخصية **(الفصل الثاني)**.

الفصل الأول

ماهية البيانات الشخصية

في ظل التطور التكنولوجي والعصر الرقمي الذي نعيش فيه تطور مفهوم البيانات الشخصية، فتعين البحث في:

- نشأة فكرة خصوصية البيانات الشخصية (**المبحث الأول**).
- ومن ثم البحث في تعريف البيانات الشخصية (**المبحث الثاني**).

المبحث الأول

نشأة فكرة خصوصية البيانات الشخصية

نظراً للارتباط الوثيق بين مفهومي الخصوصية وحماية البيانات الشخصية إذ تنبثق الثانية من الأولى، كان لزاماً على الباحث في هذا الموضع توضيح:

- نشأة مفهوم الخصوصية (**المطلب الأول**).
- وكذلك عرض المسالك المختلفة في مجال تعريف الخصوصية وكذلك نطاقها(**المطلب الثاني**).
- بالإضافة إلى البحث في ولادة وتطور مفهوم خصوصية المعلومات (**المطلب الثالث**).
- ثم عرض صور الخصوصية وبيان موقع خصوصية المعلومات بينها(**المطلب الرابع**).

المطلب الأول

نشأة مفهوم الخصوصية

حيث إن البيانات الشخصية يمكن تعريفها بشكل أدق حال الوصول إلى معنى الخصوصية، وحيث إن البيانات الشخصية تنبع من مبدأ الخصوصية، لذا وقبل الحديث عن ماهية البيانات الشخصية وجب التطرق إلى مفهوم الخصوصية في البداية.

يقصد بالخصوصية من الناحية اللغوية، حالة الخصوص، أي خص فلان بالشيء فهو يخصه خصا (بالفتح) أو خصوصا (بالضم)، وخصوصية وخصوصية (بالضم على ما يشيع وبالفتح، والفتح أفصح)، واختصه أي أفرده به دون غيره، فنقول: اختص فلان بالأمر وتخصص له إذا انفرد به[1].

والخصوص إذن الانفراد ويقابله العموم، كما يفيد الحصر وضده الإطلاق، فنقول: أعجبني هذا الصديق خصوصا، ويمتزج الانفراد والتحديد في قولنا على الخصوص أو خصوصا أي لاسيما[2].

ومن مرادفات الخصوصية في اللغة العربية، الانزواء، والانعزال والعزلة التوحد، والتفرد، والوحدة، والانطواء.

والاصطلاح المعروف في النظام القانوني الأمريكي هو اصطلاح (الخصوصية privacy)، في حين أن الاصطلاح السائد في القانون الفرنسي على وجه الخصوص، والمعبر عن ذات الحق ومرادفاته، هو اصطلاح (الحياة الخاصة La Vie privee).

---

(1) لسان العرب، ابن منظور، ط 1، منشورات مطبعة بولاق، جزء 8، ص 290. مادة: خصص

(2) قواميس اللغة: المنجد في اللغة، والوسيط، والمحيط، وفيها جميعا تطابق في بيان الدلالات اللغوية لحالة الخصوص.

ويرجع استخدام اصطلاح الخصوصية في اللغة الإنجليزية إلى القرن الخامس عشر ليدل على الحالة أو الوضع الذي يكون الفرد فيه بحال انسحاب من المجتمع فيتوارى عنهم وينأى بنفسه عن أي اهتمام من قبلهم[1].

وحقيقة إن الاصطلاح قد أدرك أول ما أدرك في اللغة الإنجليزية ليساير حقيقة أخرى وهي إن الأفكار الأولى بشأن الخصوصية أو الحالات الأولى كتطبيقات لهذا الحق (في إطار مفهوم الخصوصية المادية) ظهرت أيضا في نطاق المجتمع الإنجليزي والنظام القانوني الإنجليزي، وهو ما عزز بالتشريعات في عقدي الثمانينات والتسعينات، مثال ذلك: قانون حماية المعطيات لعام 1984 والمعدل في عام 1996.[2]

أما في الولايات المتحدة فإن الحق في الخصوصية طرح في أجواء التعديل الرابع على الدستور الأمريكي عام 1791، هذا التعديل الذي وإن كان يحصر فكرة الخصوصية في حماية منزل وذات الشخص وأوراقه، أصبح فيما بعد المصدر الدستوري للاعتراف بالخصوصية كحق عام للفرد في مواجهة أي انتهاك لشؤون حياته الخاصة، ونفس النص الدستوري استخدم أساسا لتطوير مفهوم الخصوصية وتوسيع نطاقه في النظام القانوني الأمريكي[3].

وفي المقابل، وجريا على مسلك النظام القانوني اللاتيني، ففي فرنسا

---

(1) John H.F. Shattuck، "Right of privacy" press view،1966، P2.، see also Richard A. Posner، "The Right of Privacy," 12 Georgia Law Review 393 (1977).

(2) P.johne، Invasion of Privacy Law & Legal Definition، USLegalforms.com، retrieved October،17،2013. See also Solove، Daniel J.، Marc Rotenberg، and Paul M. Schwartz (2006)، Privacy، Information، and Technology، Aspen Publishers، pp. 9–11

(3) Richard A. Posner، "The Uncertain Protection of Privacy by the Supreme court"، the supreme court review the university of chigago press، Vol. 1979، (1979)، pp. 173 - 216.

أقر المشرع تكريس مفهوم الحق في الحياة الخاصة، وحماية الحياة الخاصة كحق عام على نحو سابق من إقرار النظام القانوني الأمريكي له، غير أن ما يتعين ملاحظته أن اللغة الفرنسية تنطوي على مرادفات لتعبير الحياة الخاصة Vie privee la [1]، وتبعا لذلك فإن النظام القانوني الفرنسي ينطوي على اصطلاحات عديدة للدلالة على الخصوصية إضافة لاصطلاح الحياة الخاصة كالحق في السرية، والحق في الخلوة، والأهم الحق في الألفة الذي جرى استخدامه تشريعيا في ذات نص المادة 9 من قانون 1970 المعدل للقانون المدني الفرنسي التي كرست للاعتراف بمبدأ حماية الحياة الخاصة. [2]

ولقد سبقت الشريعة الإسلامية القوانين الوضعية في الاعتراف بالحق في الحياة الخاصة بما يزيد عن ثلاثة عشر قرنا، ولما كانت الشريعة الإسلامية عالمية، وأفصحت عن عالميتها منذ لحظاتها الأولى فإنها قادرة على استيعاب تطورات العصر وتقدمه، وذلك لمرونتها وقدرتها على التفاعل، ولعل هذا ما يتضح جليا عند المقارنة بين الشريعة الإسلامية والقانون الوضعي في مجال احترام الخصوصية أو الحياة الخاصة للإنسان، حيث نجد تفرد وتقدم الشريعة الإسلامية بصورة عملية وواقعية على الفكر القانوني المعاصر.

قد اعترفت الشريعة الإسلامية بهذا الحق ابتداء وعرفت له تطبيقات عديدة، ولعل من أبرز تطبيقات الحق في الخصوصية في الفقه الإسلامي حق الفرد في حرمة مسكنه والعيش فيه آمنا من تطفل الآخرين عليه، وهذه الحرمة قد تقررت في قوله تعالى: ﴿يَا أَيُّهَا الَّذِينَ آمَنُوا لَا تَدْخُلُوا بُيُوتًا غَيْرَ بُيُوتِكُمْ حَتَّى تَسْتَأْنِسُوا وَتُسَلِّمُوا عَلَى أَهْلِهَا ذَلِكُمْ خَيْرٌ لَكُمْ لَعَلَّكُمْ تَذَكَّرُونَ (27) فَإِنْ لَمْ تَجِدُوا فِيهَا أَحَدًا فَلَا تَدْخُلُوهَا حَتَّى يُؤْذَنَ لَكُمْ وَإِنْ قِيلَ لَكُمُ ارْجِعُوا فَارْجِعُوا هُوَ أَزْكَى لَكُمْ وَاللَّهُ بِمَا تَعْمَلُونَ عَلِيمٌ (28) لَيْسَ عَلَيْكُمْ جُنَاحٌ أَنْ تَدْخُلُوا بُيُوتًا

---

(1) isolement، réclusion، retraite، solitude

(2) Cairns، Walter. Introduction to French law (London: Cavendish، 1995(، see also West، Andrew. The French legal system 2nd ed. (London: Butterworths، 1998)

غَيْرَ مَسْكُونَةٍ فِيهَا مَتَاعٌ لَكُمْ وَاللَّهُ يَعْلَمُ مَا تُبْدُونَ وَمَا تَكْتُمُونَ (29)﴾(النور: 27 - 29)، فهذه الآية تقرر حرمة المسكن وحق الفرد في أن يتمتع وهو في مسكنه بهذه الحرمة بعيدا عن تدخل الآخرين وفضولهم.

ولذلك اعتبر الفقه الإسلامي وجود شخص في مسكن الغير دون أن يتضح قصده من الدخول ودون أن يكون هذا الدخول برضاء صاحب الحق جريمة موجبة للتعزير، ومما لا شك فيه أن حرمة المسكن تعتبر من أبرز تطبيقات هذا الحق في القانون المعاصر.

ومن تطبيقات هذا الحق النهى عن التطفل على حياة الأفراد بالمسارقة البصرية واقتحام المساكن بالنظر والاطلاع على ما يطويه الفرد عن غيره من أسرار في العادة، وقد قررت الأحاديث الكثيرة الواردة عن النبي ﷺ، ومن ذلك قوله ﷺ: (من اطلع في بيت قوم بغير إذنهم ففقؤوا عينه، فلا دية ولا قصاص) رواه أحمد والنسائي[1]

وهذه النصوص تقر حق الفرد في مقاومة الاعتداء الواقع على حياته الخاصة ودفعه؛ لأنه اعتداء على حقه في الأمن والاحتفاظ بأسراره.

ومن تطبيقات هذا الحق (الحق في الخصوصية) النهى عن التجسس على الغير، وتتبع عورات الآخرين وتعريتهم بأي وسيلة من وسائل التعرية، والذي قرره قوله تعالى: ﴿يَا أَيُّهَا الَّذِينَ آمَنُوا اجْتَنِبُوا كَثِيرًا مِنَ الظَّنِّ إِنَّ بَعْضَ الظَّنِّ إِثْمٌ وَلَا تَجَسَّسُوا﴾ [الحجرات: 12]، وروى عن النبي ﷺ قوله: (إياكم والظن فإن الظن أكذب الحديث، ولا تحسسوا، ولا تجسسوا، ولا تناجشوا، ولا تحاسدوا، ولا تباغضوا، ولا تدابروا وكونوا عباد الله إخوانا)[2].

---

(1) وَعَنْ أَبِي هُرَيْرَةَ أَنَّ النَّبِيَّ ﷺ قَالَ: مَنْ اطَّلَعَ فِي بَيْتِ قَوْمٍ بِغَيْرِ إِذْنِهِمْ فَقَدْ حَلَّ لَهُمْ أَنْ يَفْقَئُوا عَيْنَهُ رَوَاهُ أَحْمَدُ وَمُسْلِمٌ وَفِي رِوَايَةٍ: مَنْ اطَّلَعَ فِي بَيْتِ قَوْمٍ بِغَيْرِ إِذْنِهِمْ فَفَقَئُوا عَيْنَهُ فَلَا دِيَةَ لَهُ وَلَا قِصَاصَ رَوَاهُ أَحْمَدُ وَالنَّسَائِيُّ. نيل الأوطار كتاب الدماء باب من اطلع من بيت قوم مغلق عليهم بغير إذنهم.

(2) أخرجه مالك (2/907، رقم 1616)، وأحمد (2/287، رقم 7845)، والبخاري (5/1976، =

وقد نهى النبي ﷺ عن تتبع عورات الناس، فقد روي عنه أنه قال لمعاوية رضي الله عنه): (إنك إن تتبعت عورات الناس أفسدتهم أو كدت تفسدهم)[1]، وقد فسر قتادة التجسس بأنه: تتبع، أو ابتغاء عيوب الآخرين للتطلع على أسرارهم، إضافة إلى ذلك وبالاستناد إلى هذه النصوص ذهب الفقهاء إلى القول: بتحريم التجسس والتحسس أو التفتيش إلا في الأحوال المرخص بها شرعا، وتحريم التجسس والتفتيش قد ترتب عليه أنه ليس لأي إنسان سواء كان فردا أم حاكما أن يسترق السمع أو أن يتحسس ثوب الغير ليعرف ما يخفيه.

ومن تطبيقات هذا الحق أيضا حفظ الأسرار وعدم إفشائها، ولهذه الحرمة قدسية في الشريعة الإسلامية فقد روي عن النبي ﷺ أنه قال: (من حدث في مجلس بحديث فالتفت فهي أمانة)[2]، وروي عنه ﷺ قوله: (المجالس بالأمانة إلا ثلاثة: مجالس ما سفك فيه دم حرام، أو فرج حرام، أو اقتطع فيه مال بغير حق)[3].

= رقم 4849)، ومسلم (4/1985، رقم 2563)، وأبو داود (4/280، رقم 4917)، والترمذي (4/356، رقم 1988) وقال: حسن صحيح. وأخرجه أيضًا: الطبراني في الأوسط (8/222، رقم 8461)، والبيهقي.

(1) أخرج أبو داود عن معاوية بن أبي سفيان - رضي الله عنه - قال: سمعت رسول الله - ﷺ - يقول:"إنك إن تتبعتَ عوراتِ الناس أفسدتهم، أوْ كِدتَّ أن تُفسدَهم".. فقال أبو الدرداء - رضي الله عنه - : كلمة سمعها معاوية من رسول الله - ﷺ - نفعه الله تعالى بها.

(2) حدثنا أحمد بن محمد أخبرنا عبد الله بن المبارك عن ابن أبي ذئب قال أخبرني عبد الرحمن بن عطاء عن عبد الملك بن جابر بن عتيك عن جابر بن عبد الله عن النبي ﷺ قال إذا حدث الرجل الحديث ثم التفت فهي أمانة قال أبو عيسى هذا حديث حسن وإنما نعرفه من حديث ابن أبي ذئب.

(3) حَدَّثَنَا أَحْمَدُ بْنُ صَالِحٍ قَالَ قَرَأْتُ عَلَى عَبْدِ اللَّهِ بْنِ نَافِعٍ قَالَ أَخْبَرَنِي ابْنُ أَبِي ذِئْبٍ عَنْ ابْنِ أَخِي جَابِرِ بْنِ عَبْدِ اللَّهِ عَنْ جَابِرِ بْنِ عَبْدِ اللَّهِ قَالَ قَالَ رَسُولُ اللَّهِ ﷺ الْمَجَالِسُ بِالْأَمَانَةِ إِلَّا ثَلَاثَةَ مَجَالِسَ سَفْكُ دَمٍ حَرَامٍ أَوْ فَرْجٌ حَرَامٌ أَوْ اقْتِطَاعُ مَالٍ بِغَيْرِ حَقٍّ. سنن أبي داود كتاب الأدب باب في نقل الحديث.

ومـن تطبيقـات هـذا النـوع مـن الحـق (حفـظ الأسرار وعـدم إفشـائها) حـق كل واحـد مـن الزوجـين عـلى الآخـر ألا ينقـل أسراره ولا يفشـيها، والأصـل في ذلـك مـا روي عـن النبـي ﷺ أنـه قـال: (إن مـن شر النـاس يـوم القيامـة الرجـل يفـضى إلى امرأتـه، أو تفـضي إليـه ثـم ينشر سرهـا)[1].

ومـن تطبيقـات (الحـق في الخصوصيـة) أيضا حق الفـرد في المحافظة على سـمعته واعتبـاره، ومعلـوم أن الشريعـة الإسـلامية تعاقـب عـلى جريمـة القـذف في الأحـوال التـي يكـون فيهـا رمـي المجنـي عليـه مـن جنـس مـا يوجب الحـد، أمـا إذا قـام الجـاني بتوجيه كلـمات للمجنـي عليـه لا تصـل إلى حـد القـذف، ولا مـن جنـس مـا يجـب بـه القـذف، ولكنـه يعتـبر إيـذاء بأقـوال أخـرى تـؤذي المجني عليـه وتمس كرامتـه مثل: رميه بالفسـق والزندقـة ونسـبته إلى غـير الإسـلام، أو رميـه بالغبـاء والبـلادة وإيـواء اللصـوص ونحـو ذلـك، فـإن القائـل في هـذه الحالـة يكـون قـد آذى المجنـي عليـه، ولمـا كان الشـارع لم يحـدد عقوبـة لهـذه الجريمـة، فـإن العقوبـة تكـون تعزيريـة.

يضـاف إلى مـا تقـدم فـإن الشريعـة الإسـلامية قـد حمـت خصوصيـات الفـرد مـن الناحيـة الإجرائيـة، وذلـك باعتبـار هـذه الإجـراءات جـزءا مكمـلا للعقوبـات في الفقـه الإسـلامي، ويتمثـل ذلـك في: حمايـة سريـة المراسـلات، وحمايـة الفـرد مـن اسـتعمال القسـوة والعنـف في الاسـتجواب، حمايـة الفـرد مـن التعسـف في التفتيـش، حمايـة الفرد مـن الوسـائل التـي تؤثـر عـلى عقـل الإنسـان أو تكشـف عـن دروب الشـخصية).

---

(1) حدثنا محمد بن العلاء وإبراهيم بن موسى الرازي قالا أخبرنا أبو أسامة عن عمر قال إبراهيم هو عمر بن حمزة بن عبد الله العمري عن عبد الرحمن بن سعد قال سمعت أبا سعيد الخدري يقول قال رسول الله ﷺ إن أعظم الأمانة عند الله يوم القيامة الرجل يفضي إلى امرأته وتفضي إليه ثم ينشر سرها. سنن أبي داود كتاب الأدب باب في نقل الحديث.

ومـن خـلال هـذا العـرض السـابق يتضـح أن الشريعة الإسـلامية قـد اعترفت بحق الخصوصيـة منـذ اكتـمال الرسـالة، بـل إن هـذا الحـق يمثـل عنـصرا أساسـيا في منهجيتهـا، ومـن الآداب العامـة التـي تحـرص الشريعـة عـلى ضمانهـا وحمايتهـا، وأن الشريعـة قـد عرفـت تطبيقـات عديـدة لـه، أمـا عـدم اسـتعمال الفقـه الإسـلامي للفظـة (الحـق في الخصوصيـة، أو حـق الشـخصية)، فيرجـع إلى اعتبـارات عديـدة لعـل في مقدمتهـا هـو إعطـاء لفظـة الحـق تلـك الـدلالات الواسـعة.[1]

فبذلـك فـإن الخصوصيـة في نشـأتها جـاءت إنجليزية الجـذور، فتطـور مفهومها في بريطانيـا خلافـا لهـذه النشـأة المبكـرة وبقـي حبيـس المفهـوم المـادي للخصوصية، في حين أنهـا أمريكيـة التطـور، وهـي فرنسـية الاعـتراف كحـق عـام تجـاوز في نطاقـه المفاهيـم الماديـة فاحـاط بحمايـة المعنويـات وبالحمايـة مـن كافـة مظاهـر التدخل.[2]

والحـق في الخصوصيـة عميـق الجـذور مـن الوجهـة التاريخيـة[3]، ففـي الكتـب السـماوية العديـد مـن الإشـارات للخصوصيـة تنطـوي عـلى اعـتراف بحماية الشـخص من أن يكـون مراقبـا، وثمـة حمايـة للخصوصيـة في الشرائـع اليونانيـة والصينيـة القديمـة.

---

(1) Moore، Adam D. Privacy Rights: Moral and Legal Foundations (Pennsylvania State University Press، Aug.، 2010).p92 See also Lever، Annabelle. "Feminism، Democracy and the Right to Privacy." (Archove) Minerva - Journal of Philosophy See also Sprenger، Polly. "Sun on Privacy: ‹Get Over It›." Wired. January 26، 1999. P 36

(2) الدكتور محمد عبد المحسن المقاطع، حماية الحياة الخاصة للأفراد وضماناتها في مواجهة الحاسب الآلي، جامعة الكويت، بحث مقدم لمؤتمر الكويت الأول نحو صياغة جديدة لمفهوم الحياة الخاصة للأفراد وضماناتها 1992. ص 30

(3) تقرير the Electronic Privacy Information Center السنوي للأعوام 1998 - 2000 المنشور على موقعها عبر الإنترنت: http://www.privacyinternational.org/.

وقد حرم القران الكريم صراحة التجسس، وكذلك نظم حماية المساكن وحرمتها وحذر من دخول المساكن دون إذن[1].

ورحلة التطور التاريخي للحق في الخصوصية متداخلة بين هذه المراحل، وقد تأثرت بكل شيء، من مفهوم الماجنا كارتا[2] البريطاني[3].

---

(1) ﴿يَا أَيُّهَا الَّذِينَ آمَنُوا لَا تَدْخُلُوا بُيُوتًا غَيْرَ بُيُوتِكُمْ حَتَّى تَسْتَأْنِسُوا وَتُسَلِّمُوا عَلَى أَهْلِهَا ذَلِكُمْ خَيْرٌ لَكُمْ لَعَلَّكُمْ تَذَكَّرُونَ﴾ الآية 27 من سورة النور من القران الكريم، وقوله تعالى:﴿وَلَا تَجَسَّسُوا وَلَا يَغْتَبْ بَعْضُكُمْ بَعْضًا﴾ الآية 12 من سورة الحجرات.

(2) الماجنا كارتا: هي وثيقة إنجليزية صدرت لأول مرة عام 1215م. ثم صدرت مرة أخرى في القرن الثالث عشر ولكن بنسخة ذات أحكام أقل، حيث ألغيت بعض الأحكام المؤقتة الموجودة في النسخة الأولى، خصوصاً تلك الأحكام التي توجه تهديدات صريحة إلى سلطة الحاكم، وقد اعتمدت هذه الوثيقة قانوناً عام 1225م ولا تزال النسخة التي صدرت عام 1297م ضمن كتب لوائح الأنظمة الداخلية لإنجلترا وويلز حتى الآن. وقد وصفت تلك النسخة بأنها: " الميثاق العظيم للحريات في إنجلترا والحريات في الغابة". يحتوي ميثاق عام 1215م على أمور عدة منها مطالبة الملك بأن يمنح حريات معينة، وأن يقبل بأن حريته لن تكون مطلقة، وأن يوافق علناً على عدم معاقبة أي "رجل حر" إلا بموجب قانون الدولة وهذا الحق مازال قائماً حتى اليوم في هذه الدول. كانت الماجنا كارتا أول وثيقة تُفرض على ملك إنجليزي من مجموعة من رعاياه (وهم البارونات)، في محاولةً للحد من نفوذه وحماية امتيازاتهم قانونياً، ولم تكن الماجنا كارتا أول ميثاق للحد من سلطة الملك فقد سبق هذا الميثاق ميثاق آخر للحريات عام 1100م، وتأثر به تأثراً مباشراً وكان ذلك في عهد الملك هنري الأول، وبالرغم من أن للميثاق أهميةً لا يختلف عليها اثنان، فإنه بحلول النصف الثاني من القرن التاسع عشر ألغيت معظم البنود التي كانت في قالبها الأصلي، وبقيت ثلاثة بنود كجزء من قانون إنجلترا وويلز، وتعتبر عادةً كجزء من الدستور غير المدون. و في مرسوم حديث "و مثير للجدل نوعاً ما" لقوانين اللوردات، استشهد بالماجنا كارتا كمثال على لوائح أنظمة داخلية دستورية لم يمكن إلغاؤها إلا بلوائح أنظمة داخلية جديدة تنوي استبدال القديمة بقوانين أكثر وضوحًا فضلاً على أن تلغيها. كان الميثاق جزاء مهماً من عملية تاريخية ممتدة أدت إلى حكم القانون الدستوري في الدول الناطقة بالإنجليزية. بالرغم من أن الماجنا كارتا أبعد من أن تكون فريدة في شكلها أو محتواها فإنها لم تنجح في الحد من نفوذ الملك بشكل كبير عند تطبيقها في حقبة العصور الوسطى إلا أنها كانت مهمة وذات تأثير تاريخي قوي خاصة في زمن الحرب الأهلية الإنجليزية، حيث كانت رمزاً مهما عند من كانوا يتمنون أن يبرهنوا بأن الملك يقع تحت وطأة القانون. تأثر المستوطنون الأوائل في إنجلترا الجديدة بالماجنا كارتا وألهمت وثائق دستورية أتت بعدها من ضمنها دستور الولايات المتحدة.

(3) http://www.magnac.com retrived 7 - 4 - 2014

وحتـى الإعـلان العالمـي لحقـوق الإنسـان [1] وتطوراتـه عـلى مـدى الخمسـين سـنة التالية لصدوره.[2]

فبالنسـبة للماجنـا كارتـا أول مدونـة دسـتورية لحقـوق الإنسـان تتمثـل بوثيقـة الحقـوق البريطانيـة الصـادرة عـام 1215 والمعروفـة بالعهـد الأعظـم (الماجناكارتـا)[3]، وبموجبهـا تنـازل الملـك عن سـلطاته المطلقـة فمنح عهدا بعدم القبض على أحد أو حبسـه أو نفيـه أو مصـادرة أموالـه إلا بحكـم صـادر عـن سـلطة قانونيـة، واعتـبرت الماجناكارتـا مصـدرا لإطـلاق فكـرة الخصوصيـة - طبعـا لا بمعناهـا اللاحـق وإنمـا في إطـار تطبيقـات محـدودة يشـملها هذا الحـق - وكأثر للماجناكارتـا اتجهت بعـض التشريعات القديمة إلى إقرار جوانب محددة من الحق في الخصوصية، ففي عام1361 تم في بريطانيا سـن قانون

(1) الإعلان العالمي لحقوق الإنسان: هو وثيقة حقوق دولية تمثل الإعلان الذي تبنته الأمم المتحدة 10 ديسمبر 1948 في قصر شايو في باريس. الإعلان يتحدث عن رأي الأمم المتحدة عن حقوق الإنسان المحمية لدى كل الناس. الإعلان العالمي لحقوق الإنسان يتألف من 30 مادة ويخطط رأي الجمعية العامة بشأن حقوق الإنسان المكفولة لجميع الناس. يعتبر الإعلان العالمي لحقوق الإنسان سنة1948 من بين الوثائق الدولية الرئيسة لحقوق الإنسان والتي تم تبينها من قبل الأمم المتحدة، ونالت تلك الوثيقة موقعاً مهما في القانون الدولي، وذلك مع وثيقتي العهد الدولي الخاص بالحقوق المدنية والسياسية من سنة 1966، والعهد الدولي الخاص بالحقوق الاقتصادية والاجتماعية والثقافية من سنة 1966. وتشكل الوثائق الثلاثة معاً ما يسمى بـ:"لائحة الحقوق الدولية وفي 1976، بعد أن تم التصديق على الوثيقتين من قبل عدد كاف من الأمم، أخذت لائحة الحقوق الدولية قوة القانون الدولي.

(2) "The Universal Declaration of Human Rights: 1948–2008". United Nations. Retrieved 15 February 2013

(3) ثمة جدل حول اعتبار الماجناكارتا من قبيل مدونات حقوق الإنسان، لما يؤخذ عليها من أنها مدونة انتقائية سعت لحماية حقوق النبلاء والأشراف، غير أنه وبعيدا عن الغرض منها أو الظروف المرافقة، فإن انطوائها على قواعد تتصل بالحريات الإنسانية تجعل منها - خاصة بالنظر لزمن إقرارها - مدونة من بين مدونات حقوق الإنسان، والإشارة إليها في موضعنا هذا أو غيره من أبحاثنا في حقل حقوق الإنسان لا تعني القبول بحالة الانتقائية وإنما لتوظيف الأفكار والمبادئ الإيجابية التي انطوت عليها لجهة تأصيل المسائل التي تتناولها هذه الأبحاث.

The Justices of the Peace Act [1] وبموجبه تم منع اختلاس النظر واستراق السمع وعاقب عليهما بالحبس. وفي السياق نفسه وتكريسا لعدد من مظاهر الحرية أقر في عام 1629 نظام (الهايبس كاربس – Habeas - carpus) الذي قرر بعض الحقوق في التعامل مع السجناء.

وفي عام 1765 أصدر اللورد البريطاني Camden قراره في قضية Entick V. Carrington[2] بعدم جواز تفتيش منزل وضبط أوراق فيه. واعتبرت هذه القضية من أهم وأشهر القضايا الإنجليزية التي تتعلق بتفتيش الشخص وممتلكاته، وهي مقدمة المفهوم المادي للخصوصية.[3]

وقد طورت عدد من الدول حماية متقدمة للخصوصية بعد هذا التاريخ، ففي عام 1776 سن البرلمان السويدي قانون الوصول إلى السجلات العامة، والذي ألزم كافة الجهات الحكومية التي لديها معلومات أن تستخدمها لأهداف مشروعة، وسنجد هذا النضوج المبكر في النظام القانوني السويدي ذا أثر في أن تقود السويد ذاتها، في سبعينات القرن العشرين، تشريعات حماية البيانات أو تشريعات خصوصية المعلومات. [4]

---

(1) John S James and Leslie F Maxwell. A Bibliography of the British Commonwealth of Nations. Second Edition. Sweet & Maxwell. 1957. Volume 2. Page 152

See also The Justices of the Peace Act 1361، available at National Archives

(2) Entick v Carrington [1765] EWHC KB J98 is a leading case in English law establishing the civil liberties of individuals and limiting the scope of executive power. The case has also been influential in other common law jurisdictions and was an important motivation for the Fourth Amendment to the United States Constitution. It is famous for the dictum of Camden LJ: "If it is law، it will be found in our books. If it not to be found there، it is not law

(3) Kilman، Johnny and George Costello (Eds) "The Constitution of the United States of America: Analysis and Interpretation". GPO (2006).

(4) Jacobson،Amendments to the Constitution of Sweden"، Ministry =

وفي عام 1791 تم إدخال التعديلات العشرة الأولى على الدستور الأمريكي فيما عرف:(بوثيقة الحقوق)[1]، ويتصل من بينها بالحق في الخصوصية التعديلات الرابع بشكل أساسي والخامس والتاسع وما يعنينا في هذا المقام التعديل الرابع، فهذا التعديل يقرر حماية حرمة الأفراد في أشخاصهم ومساكنهم وأوراقهم وممتلكاتهم الشخصية، ويحظر تفتيشها وضبطها بصورة غير مشروعة. وكما يبدو من صراحة عبارات النص، فإن مفهوم الخصوصية الذي كرسه التعديل الرابع ينحصر في الخصوصية المادية للإنسان بمعنى الخصوصية في مواجهة الاعتداءات المادية الطبيعة التي تطال محلا ماديا(جسد الإنسان وأوراقه ومسكنه وأملاكه الخاصة).

وقد ساد هذا الفهم للخصوصية مختلف النظم القانونية لوقت طويل، لكنه اتجه إلى التطور في معظمها، كما في الولايات المتحدة وفرنسا، ليطال أبعد من ماديات الإنسان.

وفي عام 1858 منعت فرنسا نشر الحقائق الخاصة وفرضت عقابا على المخالفين، أما قانون العقوبات النرويجي فقد منع في عام1889 نشر المعلومات التي تتعلق بالشخصية والأوضاع الخاصة.[2]

ومن القضايا المهمة لخصوصية الإنترنت بشكل عام تلك العلاقة

=of justice، p 83 (2002)

(1) وثيقة الحقوق: هي اسم يجمع التعديلات العشرة الأولى لدستور الولايات المتحدة الأمريكية. قُدّمت لتهدئة مخاوف مضادي الفيدرالية الذين عارضوا المصادقات الدستورية، هذه التعديلات تضمن عدداً من الحريات الشخصية، وتحد من نفوذ الحكومة في القضاء وفي إجراءات أخرى، وتبقي على بعض النفوذ للولايات وللعامة. قدّم جيمس ماديسون التعديلات لكونغرس الولايات المتحدة الأول كسلسلة من المراسيم التشريعية. يوم وثيقة الحقوق في الولايات المتحدة الأميركية هو 15 ديسمبر.

(2) Hamilton، Alexander. Federalist Papers، #84. "On opposition to a Bill of Rights.". The Founders› Constitution. University of Chicago Press. Retrieved February 28، 2013. See also Jefferson›s letter to Madison، March 15، 1789". The Founders› Constitution. Retrieved March 9، 2013.

الدقيقـة القائمـة بـين الخصوصيـة وحمايـة البيانـات، أو بعبـارة أخـرى مـدى ضـمان مبـادئ حمايـة البيانـات كجـزء مـن الحـق الراسـخ للإنسـان في الخصوصية؛ ومـن الواضح أن ثمـة اختـلاف بـين هذيـن الأمريـن، وأن حمايـة البيانـات لا تنـدرج تماماً ضمـن مفهوم الخصوصيـة، ولكـن يمكـن أن تسـتمد أهميـة مبـادئ حمايـة البيانـات مبـاشرة مـن حـق الإنسـان في الخصوصيـة، وهـذا يلقـى مـا يدعمـه في الفقـه الـدولي، وهـو أقـل وضوحـاً مـن المبـادئ الأخـرى، وبالتأكيـد مـن الأنظمـة التـي تتبـع في توفـير حمايـة ملموسـة للبيانـات.[1]

---

(1) دراسة استقصائية عالمية حول خصوصية الإنترنت وحرية التعبير، سلسلة اليونسكو بشأن حرية الإنترنت 11/28/2013 ص10.

المطلب الثاني

تعريف الخصوصية ونطاقها

تباينت تعريفات الخصوصية فمنها ما يمكن تعريفها من الناحية الإيجابية حيث إنها الحق في الحفاظ على حرمة الحياة الخاصة، وكذلك يمكن تعريفها سلباً حيث تعتبر نقيضاً للحياة الخاصة، وإضافة إلى ذلك فتعتبر الخصوصية هي حرية الفرد في الإفصاح عن أسراره في الوقت الذي يراه مناسباً، ولمن يريد أن يفصح أمامهم عن تلك الأسرار [1]

وقد عرفت الخصوصية بأنها:

In general، the right to be free from secret surveillance and to determine whether، when، how، and to whom، one's personal or organizationalinformation is to be revealed. In specific، privacy may be divided into four categories.

1. Physical: restriction on others to experience a person or situation through one or more of the human senses;
2. Informational: restriction on searching for or revealing facts that are unknown or unknowable to others;
3. Decisional: restriction on interfering in decisions that are exclusive to an entity;

---

(1) الدكتور صالح جواد كاظم، عن التكنولوجيا الحديثة والسرية الشخصية (مباحث في القانون الدولي)، الطبعة الأولى، دار الشؤون الثقافية العامة، بغداد، 1991. ص 136.

4. Dispositional: restriction on attempts to know an individual's state of mind.[(1)(2)]

ووفقا لهذا التعريف فقد تكون الخصوصية مادية معلوماتية، أو حتى خصوصية الفرد في اتخاذ قراراته وكذلك حالته المزاجية وقراراته، وبالتالي فإن هذا التعريف يضع معنى واسعا للخصوصية، فيربطها من الناحيتين المادية المعنوية، فهي حرمة أو خصوصية الفرد في جسده، سلوكه وأفكاره.

The right to privacy is our right to keep a domain around us، which includes all those things that are part of us، such as our body، home، property، thoughts، feelings، secrets and identity. The right to privacy gives us the ability to choose which parts in this domain can be accessed by others، and to control the extent، manner and timing of the use of those parts we choose to disclose [(3)(4)].

---

(1) http://www.businessdictionary.com/definition/privacy retrived 7 - 6 - 2014

(2) Westin، A Privacy and freedom (Fifth ed.). New York، U.S.A.: Atheneum (1968) P 26. See also Johnson، Deborah (2009). Beauchamp، Bowie، Arnold، ed. Ethical theory and business. (8th ed. ed.). Upper Saddle River، N.J.: Pearson/Prentice Hall. pp. 428–442.

(3) وعلى ذلك فتعرف الخصوصية بأنها حق الأفراد أو الجماعات أو المؤسسات في أن يقرروا بأنفسهم زمن وكيفية ومدى نقل المعلومات عن أنفسهم إلى الآخرين، والخصوصية منظورا إليها من علاقة الفرد بالمشاركة الاجتماعية، هي انسحاب الفرد الطوعي والمؤقت من المجتمع العام عبر وسائل مادية أو نفسية.

(4) Yael Onn، et al.، Privacy in the Digital Environment، Haifa Center of Law & Technology، (2005) pp. 1 - 12

وقد ذهب Brandeis وWarren في عام 1890 إلى أن تعريف الخصوصية بأنها: (الحق في أن يترك الشخص وحيدا)، ولهذا فإن الخصوصية وفق هذا الفهم تعدو أهم سمة من سمات الحرية في المجتمع الديمقراطي.(1)

وفي سياق هذا التعريف الذي وإن كان في ظاهر عباراته يركز على فكرة العزلة التي تعد جوهر الخصوصية المادية، فإنه يقرن الخصوصية بالحرية عوضا عما ينطوي عليه - وفق تحليل الفقيهين ذاتهما - على تكريس فكرة الحق في السرية الذي يعد جوهر حماية الخصوصية المعنوية.

وتكريسا للربط بين الخصوصية والحرية، بل بتجاوز لنطاق الربط إلى حد الخلط بين مفهومي الحرية والخصوصية، ثمة اتجاه عريض ذهب في تعريفه للخصوصية إلى تكريس عناصر الحق في الحرية التي ينطوي عليها، ومن ذلك ما قال به الفقيه John Shattuck: إن الحياة الخاصة لا تعني فقط الحق في أن يظل المرء بعيدا عن تطفل الآخرين، ولكنها تتسع لأكثر من ذلك، إنها تعني: (أن يعيش الشخص كما يحلو له أن يعيش، مستمتعا بممارسة أنشطة خاصة معينة، حتى ولو كان سلوكه على مرأى من الناس، فالإنسان حر في ارتداء ما يراه مناسبا، وحر في أن يظهر بهيئة تتميز بها شخصيته، أو أن يركب الدراجة البخارية بدون ارتداء الخوذة الواقية للرأس).(2)

---

(1) Samuel Warren and Louis Brandeis، law review article،1890 Harvard Law Review. See also Susan E. Gallagher، Introduction to "The Right to Privacy" by Louis D. Brandeis and Samuel Warren: A Digital Critical Edition، University of Massachusetts Press، forthcoming. See also Dorothy J. Glancy، "The Invention of the Right to Privacy"، Arizona Law Review، v.21، n.1، pp.1 - 39 (1979)، p.1 ("The right to privacy is، as a legal concept، a fairly recent invention. It dates back to a law review article published in December of 1890 by two young Boston lawyers، Samuel Warren and Louis Brandeis.").

(2) John Shattuck،Rights of Privacy،National Textbook Co.، 1977 p 12 - 24

وهـذا التصـور هـو مـا ذهـب إليـه أيضـا القـاضي الأمريـكي (دوغـلاس)، فقـد ذكر أن الحـق في الحيـاة الخاصـة هـو: (حـق الفـرد في أن يختـار سـلوكه الشـخصي وتصرفاتـه في الحيـاة عندمـا يشـارك في الحيـاة الاجتماعيـة مـع الآخريـن) [1]، ثـم حـدد دوغـلاس ثـلاث مجموعـات رئيسـة لهـذا الحـق وهـي: 1 - حريـة التعبير عـن الأفـكار والاهتمامات والـذوق والشـخصية.2 - حريـة أن يكـون لديـه أولاد يربيهـم وينشـئهم 3 - حـق الفـرد في كرامـة بدنـه وتحـرره مـن القسـر والقهـر.[2]

وبالنسـبة للقانـون الفرنـسي فيعـرف الحيـاة الخاصـة تعريفـا ذا صلـة بفكـرة الحريـة، حيـث يـرى أن الحيـاة الخاصـة: (هـي مجمـوع الحـالات والأعـمال والآراء الصـادرة عـن الفـرد بحريـة، والتـي لا ترتبـط بـأي التـزام في مواجهـة الآخريـن)، ويعترف القانـون المـدني الفرنـسي بالحـق في الخصوصيـة في المـادة التاسـعة مـن القانـون.

حيـث تنص المادة التاسـعة على: [3]

"Everyone has the right to respect for his or her private life"

و قـد أكـدت الفقـرة الثانيـة مـن المـادة ذاتهـا عـلى اتخاذ مـا يجـب مـن إجراءات لمنـع التعـدي عـلى الخصوصية.[4]

---

(1) Kalman، Laura; Garrow، David "Review: The Promise and Peril of Privacy". Reviews in American History (The Johns Hopkins University Press) (1994). p 22 See also Loewy، Arnold H. (2003). "Morals Legislation and the Establishment Clause". Alabama Law Review 55 (1): 159–182

(2) A. Westin،، Privacy and Freedom، New York: Atheneum. 1967، p 23

(3) Article 9 of the French Civil Code، inserted by Act of Parliament of 17 July 1970

(4) Elliott، Catherine. French legal system (Harlow، England: Longman، 2000) p 45 See also Bell، John. Principles of French law (Oxford ; New York: Oxford University Press، 1998)See also Reynolds، Thomas. Foreign law: current sources of codes and basic legislation in jurisdictions of the world (Littleton، Colo.: F.B. Rothman، 1989 -

أمـا في نطـاق التعريفـات التـي لم تصـل في نطاقهـا حـد التعريفـات المتقدمـة مـن حيـث الاتسـاع، بـل عكسـت مفهـوم الخصوصيـة كحـق مسـتقل يحمـي الفـرد مـن الاعتـداءات المادية والمعنويـة التـي تطـال حياتـه الخاصـة، فنجـدEdward Bloustein يذهـب إلى أن الخصوصيـة هـي: الحـق في حمايـة الشـخصية، ومنـع الاعتـداء عليهـا، واسـتقلال الأفـراد وكرامتهـم وسـلامتهم [1]، وفي السـياق ذاتـه، ووفقـا لـ Gavison Ruth فـإن للخصوصيـة ثلاثـة عنـاصر: السريـة Secrecy والعزلـة Solitude والتخفـي أو التسـترAnonymity.

أمـا لجنـة CALCUTT المشـكلة في بريطانيـا بعـام 1970 بشـأن تقييـم الحاجـة لتشريـع لحمايـة الخصوصيـة، فقـد قالـت: إنهـا لم تتمكـن مـن الوصـول إلى تعريـف كافٍ ومقبـول للخصوصيـة، لكنهـا رغـم ذلـك تبنـت تعريفـا قانونيـا ضمنتـه تقريرهـا حـول الخصوصيـة وهو:(حـق الأفـراد في الحمايـة ضـد التدخـل في الحيـاة الخاصـة وشـؤونهم وشـؤون عائلاتهـم بوسـائل ماديـة مبـاشرة أو عـن طريـق نـشر المعلومـات عنهـم).[2]

مـن هـذه التعريفـات يمكننـا إيجاز الحقائـق التاليـة المتصلة بتحديـد ماهية الحق في الحيـاة الخاصة ونطاقه:

أولا: مـن الصعـب وضـع تعريـف جامـع للحـق في الحيـاة الخاصـة (بالفرنسـية 'Lavie Privee') أو الخصوصيـة سـندا للاصطـلاح المسـتخدم في الفقـه الأنجلـو الأمريـكي (Privacy)، لأن تعريـف هـذا الحـق يرتبـط في الحقيقـة بمنظومـة: " التقاليـد والثقافـة والقيـم الدينيـة السـائدة والنظـام السـياسي في كل مجتمـع".

(1) Bloustein، Edward J،Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser;N.Y. U Law review (1964) p11

(2) تقرير الخصوصية لعام 2000 - المرجع السابق ص 4.

ثانيا: أمام صعوبة وضع تعريف إيجابي للحق في الحياة الخاصة، اتجه جانب من الفقه إلى صك تعريف سلبي، يحدد المقصود بالحق في الحياة الخاصة بكل ما لا يعد من حياة الفرد العامة، غير أن هذا المسلك منتقد من وجوه عدة أهمها صعوبة التمييز بين ما يندرج ضمن مفهوم الحياة العامة وذلك الذي يقع ضمن نطاق الحياة الخاصة ومثال ذلك: الحياة المهنية التي تعد لدى البعض مما يدخل في نطاق الحياة العامة ولدى آخرين مما يعد من صميم الحياة الخاصة".

ثالثا: يستخلص جانب من الفقه [1]عناصر رئيسة للحق في الحياة الخاصة تلتقي عندها - كحد أدنى - الآراء المتباينة بشأن تعريف هذا الحق، أولها: "اقتران الخصوصية بالانسحاب من الوسط أو العالم المحيط، وربطها من ثم بفكرة الخلوة أو العزلة "، وسندا لذلك تتمثل غاية هذا الحق - كما يحددها الأستاذ (Kayser P.) - بضمان السلام والسكينة لهذا الجانب المنعزل من الحياة غير المتصل بالأنشطة العامة بجعله بمنأى عن التقصي والإفشاء غير المشروعين. "وثانيهما:"الاعتراف للشخص بسلطة الاعتراض على التدخل أو التقصي عن خصوصياته من جهة وسلطة الاعتراض على وصول معلومات تتعلق بخصوصياته إلى الغير من جهة أخرى".

---

(1) يقول د. هشام رستم: " إن للخصوصية وجهين متمايزين، مادي، وقوامه عدم إقحام النفس في خصوصيات الآخرين والتدخل في شؤونهم الخاصة، والخصوصية، منظورا إليها من هذه الوجهة، مادية physical privacy حسب الوصف الذي يطلقه عليها البعض، والثاني إعلامي: ومقتضاه ألا تكون الشؤون الخاصة بالفرد محلا للحق في الإعلام بالنسبة للغير، وهو ما يستتبع عدم استخدام الآخرين معلومات تتعلق بحياة الفرد الخاصة، والخصوصية من هذا الوجه - كما يسميها البعض - إعلامية Informational Privacy.(د.هشام فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة، أسيوط،1992)

المطلب الثالث

ولادة وتطور مفهوم خصوصية المعلومات

إن أول حقيقة تاريخية ننطلق منها ونكرسها في هذا المقام إن فكرة الخصوصية وارتباطها بتقنية المعلومات هي أول مسائل قانون الكمبيوتر عموما من الوجهة التاريخية، وهي أول مناطق التساؤل عن أثر التقنية على النظام القانوني ومسائله، وقد انطلقت في الستينات وفي أجواء التطور التكنولوجي الواسع، وأجواء الاستخدامات المتزايدة للحوسبة وإنشاء بنوك المعلومات وعمليات المعالجة الآلية للبيانات، وفي سياق حماية الأفراد من مخاطر التقنية التي تتهدد حياتهم الخاصة، فتمس على نحو مباشر خصوصياتهم وأسرارهم، ولهذا ارتبطت ولادة مفهوم خصوصية المعلومات بالخشية من مخاطر التقنية ذاتها.

إن الدراسات القانونية الأكاديمية التي عنيت بالخصوصية وبحقوق الإنسان في ضوء التطورات التقنية محدودة بشكل عام، ويمكن القول: إن نهاية الستينات والسبعينات شهدت انطلاق مثل هذه الدراسات، وإن هذه الفترة تحديدا هي التي أثير فيها لأول مرة وبشكل متزايد مفهوم خصوصية المعلومات كمفهوم مستقل عن بقية مفاهيم الخصوصية وتحديدا التدخل المادي ومسائل الرقابة، ويعزى الفضل في توجيه الانتباه لمفهوم خصوصية المعلومات في هذه الفترة إلى مؤلفين أمريكيين مهمين في هذا الحقل:

- **الأول:** كتاب الخصوصية والحرية Privacy and Freedom لمؤلفه ويستن Alan Westin عام 1967 [1].

والثاني: كتاب الاعتداء على الخصوصية The Assault on Privacy

---

(1) Westin، A F، "Privacy and Freedom"، New York، Atheneum. (1967) p. 18.

لمؤلفه ميلر Miller [1]، وكليهما قدم مفهوما وتعريفا لخصوصية المعلومات.

فوفقا لـ (ويستن) فإن خصوصية المعلومات تعني: " حق الأفراد في تحديد متى وكيف وإلى أي مدى تصل المعلومات عنهم للآخرين".

the claim of individuals 'to determine for themselves when، how and to what extent information about them is communicated to other

في حين جاء تعريف ميلر أكثر عمقا - مع أن ويستن يعتبر منظر الحق في خصوصية المعلومات - إذ عرف خصوصية المعلومات بأنها: "قدرة الأفراد على التحكم بدورة المعلومات التي تتعلق بهم".

'the individual's ability to control the circulation of information relating to him'

فإذا تجاوزنا فكرة تحديد المعنى وتأصيله، نجد أن كتاب قواعد الحياة الخاصة والرقابة العامة Private Lives and Public Surveillance لمؤلفه Rule والمنشور في عام 1973[2] قد استعرض على نحو شامل ومعمق مسائل جمع واستخدام البيانات الشخصية كوسيلة للسيطرة الاجتماعية، وتضمن تفاصيل حالات تطبيقية ودراسية لعدد من الهيئات والقطاعات كنظام ترخيص السائقين البريطاني - UK Driver Licensing system، ونظام تقارير ائتمان المستهلكين الأمريكي - US Consumer Credit Reporting، تضمنت بحث ما تقوم هذه الأنظمة بجمعه من بيانات، ووسائل الجمع، ومن له حق الوصول لها، وكيف تستخدم، وكيف يؤثر هذا الاستخدام على صاحب البيانات.

---

(1) Miller، A، “The Assault on Privacy”، Ann Arbor، University of Michigan Press، (1971)p.40.

(2) Rule، J B،” Private Lives and Public Surveillance”، London، Allen Lane، (1973) p.33.

ومما سبق، يمكن القول إن الخصوصية من حيث مفهومها جرى التعامل معها كحق لمنع إساءة استخدام الحكومة للبيانات التي يصير معالجتها آليا أو إلكترونيا أو تقييد استخدامها وفق القانون فقط.

وفي أمريكا وأوروبا معا، جرى تطوير هذه الفكرة ضمن حزمة شاملة من مبادئ السلوك والممارسات المقبولة، أهمها تأكيد الاستخدام العادل والمنصف للبيانات الشخصية، والتدخل بالحدود الدنيا، وتقييد وتضييق أغراض استخدام البيانات، وحصر الاستخدام في غرض الجمع.

وقد كان للتطورات التقنية، وتحديدا إنشاء بنوك المعلومات وإجراء عمليات المعالجة والتحليل بواسطة الكمبيوترات، الأثر في خلق مفهوم خصوصية المعلومات بالمحتوى المشار إليه، خاصة في هذه الدراسات الأكاديمية، وقد كان الفقهاء المتقدم الإشارة إليهم (وسيترن وميلر وورولي) من أوائل من ساهموا في إثارة مسائل نظام خصوصية المعلومات وتوضيح ملامحه.

وفي الفترة ذاتها، قامت الدول الغربية بسن تشريعات حماية البيانات، مثال ذلك التوجيه الأوروبي الصادر بشأن حماية البيانات (Data Protection Directive)[1] [2] انطلاقا من مطلع التسعينات، وترافق

---

(1) The Data Protection Directive (officially Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data) is a European Union directive adopted in 1995 which regulates the processing of personal data within the European Union. It is an important component of EU privacy and human rights law. On 25 January 2012، the European Commission unveiled a draft European General Data Protection Regulation that will supersede the Data Protection Directive>

(2) Julia M. Fromholz، The European Union Data Privacy Directive، Berkeley Tech. (2000) p 23 See also Dean William Harvey & Amy White، The Impact of Computer Security Regulation on American Companies، 8 Tex. Wesleyan L. Rev (2002) And see Kamaal Zaidi، Harmonizing U.S. - EU Online Privacy Law: Toward a U.S. Comprehensive Regime For the Protection of Personal Data، 12 Mich.St. J. Int'l L. 169 (2003).

ذلك مع دراسات مقارنة بين القوانين الوطنية، وفي هذا الصدد يبرز مثلا جهد الكاتب بوركرت Burkert[1] وناغتر Nugter[2] خلال الثمانينات وبداية التسعينات.

وقد شهد عام 1994 إعداد دراسات واسعة بشأن المسائل المتصلة بالخصوصية وحقوق الإنسان عالميا في ضوء التطورات التقنية الحديثة، منها مثلا: الدراسة التي أعدها البروفسور ميشيل Michael بعنوان:(الخصوصية وحقوق الإنسان - Privacy and Human Rights)[3]، تحت إشراف اليونسكو، حيث قام المؤلف بتقييم المحتوى الاجتماعي والسياسي والثقافي المتضمن في تشريعات الخصوصية وحماية البيانات عالميا.

وبتفاصيل أقل مما ورد في دراسات ميلر وويستن السابق الإشارة إليهما. والمفيد في مؤلف ميشيل أنه استعرض الصعوبات والتباينات الثقافية في استخدام اصطلاح الخصوصية واختلاف المفهوم القانوني أيضا للخصوصية بين النظم القانونية المختلفة وفي نطاق المفهوم القانوني للخصوصية أوضح هذا المؤلف ثلاثة مواقف: (موقف مؤتمر دول الشمال الأوروبي، موقف نظام القانوني المدني - اللاتيني، وموقف نظام القانون العام - الأنجلوأمريكي) فعرض في نطاق المفهوم الأول، موقف لقاء الخبراء القانونيين في ستوكهولم

(1) Burkert، H، Institutions of Data Protection: An Attempt at a Functional Explanation of European National Data Protection Laws. Computer Law Journal، (1982)، 3 (2)، p.167.

(2) Nugter، A.C.M. Transborder flow of personal data within the EC. Boston: Kluwer، (1990) p.90.

(3) Michael، J، "Privacy and Human Rights: An International and Comparative Study with Special Reference to Developments in Information Technology"، Dartmouth. (1994) p.45

عـام 1967 الـذي نتج عنـه إعـلان غـير ملـزم حـول معنـى الحـق في الخصوصيـة تضمـن المبـادئ التـي قـام عليهـا فيـما بعـد أول تشريـع شـمولي لحمايـة البيانـات وهـو القانـون السـويدي لعـام 1973.

وقـد اعتـبر هـذا الإعـلان خصوصيـة المعلومـات مزيـج مـن مكنـات أو حقـوق الأفـراد مـن خـلال التـوازن بـين الحـق في الوصـول للمعلومـات والتنظيـمات الإداريـة لملفـات الكمبيوتـر

a combination of legal remedy available to the individual through rights of access and the administrative regulation of computerized records

والحـق في الوصـول للمعلومـات مقـرر في عـدد مـن الـدول منـذ القـدم، ففـي السـويد اقـر هـذا الحـق بموجـب قانـون حريـة الصحافـة لعـام 1776 الـذي يعـد أقـدم قانـون للوصـول للمعلومـات في العـالم، ومـن جديـد تعـود السـويد لتكـون أول دولة تضع قانونـا لتنظيـم سـجلات الكمبيوتـر وحمايـة البيانـات، وتقـود موجـة التشريـع في هـذا الحقـل مـن خـلال قانـون عـام 1973[1] بشـأن حمايـة البيانـات.[2]

أمـا الفهـم القائـم في نظـام القانـوني المـدني، فإنـه مختلـف، وذلـك لقيامـه عـلى إقـرار المبـدأ العـام، وهـذا ملحـوظ بالأسـاس مـن خـلال الموقـف الأوروبي الـذي يظهـر أفضـل مـا يظهـر مـن اتفاقيـة حقـوق الإنسـان الأوروبيـة، وهـو الفهـم الـذي تقـارب معـه الموقـف الأمريـكي - رغـم انتمائـه لطائفـة القانـون العـام - عندمـا جـرى توسـيع القواعـد الدسـتورية والمبـادئ الدسـتورية العامـة لحمايـة طائفة من الحقـوق، كالحق في الخصوصيـة مـن أنشـطة الرقابـة الحكوميـة متـى مـا توفـر للفـرد اعتقـاد وتوقـع مقبـول بخصوصيتـه.

---

(1) The law text available at http://itlaw.wikia.com/wiki/Category:Legislation - Sweden - Privacy retrived 7 - 6 - 2014

(2) Cavoukian، Ann Who Knows: Safeguarding Your Privacy in A Networked World Random House of Canada: (1995).P 46

وإذا كان القانون المدني – اللاتيني – يقوم في تعامله مع الخصوصية ومفهومها على أساس المبدأ، فإن القانون العام يطبق مبادئ الحماية وفق الحالات الفردية، ففي بريطانيا مثلا والتي تمثل بوضوح هذا النظام، فإن المكنات التي اعترف بها القضاء - بعيدا عن تدخل المشرع - والحقوق التي أقرت كانت تتعلق بحقوق خاصة في حالات انتهاكات واعتداءات خاصة، وكان إقرار الحق يعتمد على مكنات قانونية متباينة، كقانون السرية أو نصوص القذف والتشهير وغيرها - ليس من بينها القول صراحة باستنادها إلى مبدأ حماية الخصوصية - وهذا ما يفسر عدم ورود هذا المفهوم نفسه في قانون حماية البيانات البريطاني الأخير لعام 1998 وسابقه 1984، فكلاهما لا يقيمان مفهوم مبدأ حماية الخصوصية صراحة، وإن كانا ينظمان مبادئ حماية البيانات الخاصة والتعامل معها.

ومع أن مجموعة قوانين جديدة منذ عام 1998 في بريطانيا أوجبت تطوير مفهوم الخصوصية كقانون حماية البيانات لعام [(1)]98، وقانون حقوق الإنسان 98، وقانون حرية الوصول للمعلومات لعام 98 أيضا، وبرغم اعتراف المادة 8 من قانون حقوق الإنسان بالحق في الخصوصية، فإن هذا التطوير لم يصل إلى إقرار المبدأ ونطاقه ومقتضياته بالقدر المقرر في بقية التشريعات الأوروبية، وفيما اعتمدت عليه هذه القوانين من الأدلة والقرارات الصادرة عن الاتحاد الأوروبي.[(2)]

إذن فقد تطور الحق في الخصوصية وحماية البيانات في الستينات

---

(1) Hoffman، David; Rowe، John،Human Rights in the UK: an Introduction to the Human Rights Act 1998 (2nd ed.). Harlow، United Kingdom (2006). P 23 See also Amos، Merris،"Transplanting Human Rights Norms: The Case of the United Kingdom›s Human Rights Act". Human Rights Quarterly (2013).

(2) Warren and Brandeis، "The Right To Privacy"، 4 Harvard Law Review 193 (1890) p 39

والسبعينات نتيجة للتأثر بتقنية المعلومات وبسبب القوى الرقابية المحتملة لأنظمة الكمبيوتر التي استوجبت وضع قواعد معينة تحكم جمع ومعالجة البيانات الخاصة، وفي هذا الحقل فإن من المهم الإشارة إلى أن أول معالجة تشريعية في ميدان حماية البيانات كان عام 1970 في ولاية هيس بألمانيا(LAND OF HESSE IN GERMANY)، لكن هذه المعالجة لا تعد قانونا متكاملا لاعتبارات عديدة أولها: أنه ليس قانون دولة،[1] وقد تبعه سن أول قانون وطني(متكامل) في السويد عام 1973، ثم الولايات المتحدة عام 1974، ثم ألمانيا على المستوى الفدرالي عام 1977، ثم فرنسا عام 1978.

وفي عام 1981 وضع مجلس أوروبا اتفاقية حماية الأفراد من مخاطر المعالجة الآلية للبيانات الشخصية، ووضعت كذلك منظمة التعاون الاقتصادي والتنمية دليلا إرشاديا لحماية الخصوصية ونقل البيانات الخاصة، والذي قرر مجموعة قواعد تحكم عمليات المعالجة الإلكترونية للبيانات.

وهذه القواعد تصف البيانات والمعلومات الشخصية على أنها معطيات تتوفر لها الحماية في كل مرحلة من مراحل الجمع COLLECTION والتخزين STORAGE والمعالجة PROCESSING والنشر DISSEMINATION.

ثم وفي خطوة متطورة على المستوى التشريعي الإقليمي، بل وذات أثر عالمي، أصدر الاتحاد الأوروبي الأمر التشريعي الخاص بحماية البيانات

(1) Modernisierung des Datenschutzes: Öffentliche Anhörung des Innenausschusses (Modernisation of the data security:Public hearing of the interior committee)، 6 March 2007، available at http://www.bundestag.de/aktuell/archiv/2007/innen_kw10/index.html> See also M.juien، Constitutional Privacy and Data Protection Framework retrived 8 - 6 - 2014 https://www.privacyinternational.org/reports/germany/i - legal - framework

ونقلها عبر الحدود لعام [1] 1995، الذي مثل مرحلة جديدة في إعادة تنظيم خصوصية المعلومات والذي أدى إلى إعادة وضع العديد من دول أوروبا تشريعات جديدة، أو تطوير تشريعاتها القائمة في هذا الحقل، بل أثر فيما تضمنه من معايير في حقل نقل البيانات خارج الحدود لجهة سعي العديد من دول العالم خارج نطاق أوروبا إلى الاقتضاء بهذا القانون.

وبالعموم يمكننا القول بإيجاز: إن مفهوم حماية البيانات في المواثيق المتقدمة يتطلب أن تكون البيانات الشخصية: [2]

1 - قد تم الحصول عليها بطريق مشروع وقانوني.

2 - تستخدم للغرض الأصلي المعلن والمحدد، ولا تكشف لغير المصرح لهم بالاطلاع عليها.

3 - تتصل بالغرض المقصود من الجمع ولا تتجاوزه ومحصورة بذلك.

4 - صحيحة وتخضع لعمليات التحديث والتصحيح.

5 - يتوفر حق الوصول إليها، مع حق الإخطار بأنشطة المعالجة أو النقل وحق التصحيح والتعديل وحتى طلب الإلغاء.

6 - تحفظ سرية وتحمى سريتها وفق معايير أمن ملائمة لحماية المعلومات ونظم المعالجة.

7 – تتلف عند استنفاذ الغرض من جمعها.

---

(1) Quinn، Michael J. Ethics for the Information Age، U.Y.E pub، (2009). P 56 See also Westin، A. (1968). Privacy and freedom (Fifth ed.). New York، U.S.A.: Atheneum

(2) Johnson، Deborah، Beauchamp، Bowie، Arnold، ed. “Ethical theory and business”. (8th ed.) Upper Saddle River (2009) p. 33 See also Etzioni، Amitai "The Privacy Merchants: What is to be done?". The Journal of Constitutional Law (March 2012).

إذن يمكـن القـول: إن خصوصيـة المعلومـات هـي حمايـة البيانـات، لكـن الخصوصيـة ليسـت هـي حمايـة البيانـات، فالأخـيرة شيء مـن الخصوصيـة وتتعلـق بمواجهـة الاعتـداءات عـلى البيانـات الشـخصية، وتنظيـم الحـق في البيانـات الشـخصية وسـيطرة صاحبهـا عليهـا، في حـين أن الخصوصيـة عـلى إطلاقهـا، تنطـوي عـلى خصوصيـة البيانـات، وخصوصيـة الاتصـالات في مواجهـة أنشـطة الرقابـة والتجسـس، وخصوصيـة المـكان وحرمتـه في مواجهـة أنشـطة الاعتـداء الماديـة، وهـي مسـائل حرمـة المسـكن وحرمـة الشـخص مـن التفتيـش غـير القانـوني، وأيضـا خصوصيـة المراسـلات ومـن ضمنهـا مراسـلات ماديـة وأخـرى إلكترونيـة، وغـير ذلـك مـن أوجـه الحمايـة ذات الطبيعـة أو المحتـوى المـادي أو المعنـوي، ولا يعنـي قولنـا هـذا تقسـيم الحـق في الخصوصيـة، فهـو بوصفـه الحـق الـذي تحمـى فيـه حيـاة الفـرد الخاصـة مـن كل اعتـداء وتطـاول وانتهـاك أو تدخـل، مـادي أو معنـوي، ولهـذا فهـو يشـمل هـذه المظاهـر وغيرهـا دون أن ينتقـص ذلـك مـن كونـه حقـا موحـدا مسـتقلا.

فالخصوصيـة بالعمـوم تنطـوي عـلى حمايـة مظاهـر ماديـة ومعنويـة ومعلوماتيـة ولا تقـف عنـد حمايـة البيانـات الشخصية، وبالتـالي مـن المهـم إدراك أن الـترادف بوجـه عـام قائـم مـا بـين اصطـلاح خصوصيـة المعلومـات وحمايـة البيانـات، وليـس بـين الخصوصيـة وبـين حمايـة البيانـات.

أمـا شـيوع اسـتخدام اصطـلاح الخصوصيـة مسـتقلا ومنفـردا دون إلحاقـه بالبيانـات في البيئـة الإلكترونيـة للدلالـة عـلى حمايـة البيانـات واسـتخدامه كذلـك في الدراسـات الأكاديميـة وفي الدراسـات التقنيـة وأبحـاث وتقريـر قطاعـات الأعـمال، فهـو أمـر يرجـع إلى أن تعبـير الخصوصيـة شـاع بوقعـه هـذا في ظـل تزايـد مخاطـر التقنيـة إلى مـدى ارتبـط بهـا في الاسـتخدام وكأنـه ينحـصر في نطاقهـا وبيئتهـا، وهـو طبعـا ليـس كذلـك، لكـن ربمـا لأن أشـد مـا يمكـن أن يمثـل تغـولا عـلى هـذا الحـق وانتهـاكا لـه، هـي الوسـائل التقنيـة ومخاطـر المعالجـة الآليـة للبيانـات.

كـما أن اسـتخدام اصطـلاح الخصوصيـة في بيئـة مواقـع الإنترنـت ومسـائل

عقـود التقنيـة أو خدمـات التقنيـة عمومـا يشـير إلى حمايـة الخصوصيـة المعلوماتيـة أو حمايـة البيانـات.

إن الحـق في الخصوصيـة أصبـح مـن الحقـوق المعـترف بها عالميـا، وتعتـبر البيانات الشـخصية جـزءا مـما تشـمله حمايـة الخصوصيـة وقـد أصبـح الحـق في حمايـة البيانـات الشـخصية حـق أصيـل لـكل شـخص طبيعـي كان أو اعتبـاري، لقـد أقـرت كثـير مـن دول العـالم قوانـين لحمايـة الخصوصيـة وحمايـة البيانـات الشـخصية.[1]

إن الحـق في الخصوصيـة يعتـبر مبـدأ حديثـا نسـبيا وقـد تم تعريفـه في عام 1890 بأنـه: "the right to be left alone". الحـق في الخلـوة، فهـو يعـبر عـن حـق الشـخص في الابتعـاد عـن النـاس حيـث يعيـش بعيـدا عـن قيـود الحيـاة الاجتماعيـة فمـن حـق الشـخص أن يسـتلزم مـن الغـير أن يتركـوه وشـأنه، ولا يعكـر عليـه أحـد صفـو خلوتـه [2] هـذا التعريـف - الكلاسـيكي كان نتيجـة للتعديـات الصحفيـة في ذلـك الوقـت.[3]

في عـام 1960 امتـد هـذا المفهـوم القانـوني للخصوصيـة لتشـمل الحمايـة ضـد تدخـل الحكومـة في قـرارات شـخصية مثـل وسـائل منـع الحمـل والإجهـاض.[4]

وقـد أدى ظهـور مجتمـع المعلومـات إلى تغيـير تفاسـير الحـق في الخصوصيـة إلى "حـق الفـرد في التحكـم في تـداول المعلومـات المتعلقـة بـه أو لـه. هـذا التعريـف

---

(1) Etzioni، ACommunitarianism. In B. S. Turner (Ed.)، The Cambridge Dictionary of Sociology Cambridge، UK: Cambridge University. (2006). (pp. 81 - 83).

(2) Warren، S. D، and Brandeis، L. D، "The right to privacy"، Harvard Law Review، (1890) p.56.

(3) Shade، L. R،Reconsidering the right to privacy in Canada. Bulletin of Science، Technology & Society،. (2008). p 80 - 91

(4) Amitai Etzioni،، The Limits of Privacy، New York: Basic Books. 2000،p 60

الحديث ينطوي على علاقة وثيقة بين الخصوصية والبيانات الشخصية، على الرغم من أن حماية البيانات الشخصية ليست مطابقة لحماية الخصوصية. " خصوصية المعلومات"[1].

في عام 1984م صدر الإعلان العالمي لحقوق الإنسان، وذكر في مادته الخامسة عشرة: "لا يُعرَّض أي شخص لتدخل تعسفي في حياته الخاصة أو أسرته أو مسكنه أو رسائله، أو شن حملات على شرفه وسمعته، ولكل شخص الحق في طلب حماية القانون له من مثل هذه التدخلات أو تلك الحملات".[2]

وفي عام 1858م قامت الحكومة الفرنسية بإصدار قرار يُمنع فيه نشر الحقائق المتعلقة بخصوصية الأفراد، بجانب فرض العقوبات لمن يقوم بمخالفة أمر هذا القرار. وفي ميثاق الحقوق الأساسية للاتحاد الأوروبي، ذكرت المادة السابعة من الميثاق: "أن لكل شخص الحق في أن تُحتَرم حياته الخاصة وحياته العائلية وبيته واتصالاته".

وقامت منظمة التعاون الاقتصادي والتنمية بوضع آلية (دليل إرشادي)، لحماية البيانات الشخصية وطرق نقلها، ووضع ضوابط تحكم عملية المعالجة الإلكترونية لها، وتوفر لها الحماية في مراحل التجميع والتخزين والمعالجة والنشر، على أن تكون هذه البيانات الشخصية: تم الحصول عليها بطريقة شرعية وقانونية، وتستخدم للغرض الذي جمعت له والمعلن عنه، وتكون صحيحة وتخضع لعمليات التحديث والتصحيح، وتوفر القدرة على

---

(1) Ruth Gavison، "Privacy and the Limits of the Law،" in Michael J. Gorr and Sterling Harwood، eds.، Crime and Punishment: Philosophic Explorations (Belmont، CA: Wadsworth Publishing Co.، 2000، formerly Jones and Bartlett Publishers، 1996)، pp. 46-68.

(2) Phillips، Melanie "From human rights to the EU، the tide›s turning against the liberal thought police". Daily Mail (London). (4 July 2011).p 72

حفظ سريتها وحماية الوصول إليها، والقدرة على إتلافها بعد انتهاء الغرض من جمعها.[1]

وقد أثرت هذه الآلية في كثير من التشريعات الوطنية، في حفظ خصوصية البيانات الشخصية للأفراد، حتى خارج إطار الدول الأعضاء في هذه المنظمة.[2]

إن من الصعوبة القيام بوضع تعريف جامع للخصوصية، وذلك لارتباطها بالانتماءات الدينية والعادات والقيم في المحيط الذي يعيش فيه الشخص، فنجد أنه في التشريعات والقوانين الدولية لا يُذكر فيها تعريف معين للخصوصية، وإنما تكتفي بوضع نصوص تكفل حماية هذا الحق وتعدِد صور الاعتداء عليه. قد تعتبر قوانين حفظ الخصوصية في العديد من الدول محدودة المجال، فعلى سبيل المثال:القوانين المرتبطة بتحصيل الضرائب، والتي تتطلب عادةً مشاركة البيانات الشخصية المالية من إيرادات وديون.

وقد تتعارض قوانين حفظ الخصوصية في بعض الدول مع قوانين حرية التعبير ويصف بعض الباحثين الاقتصاديين وعلماء النفس بأن الإفصاح عن بعض المعلومات الشخصية، لهدف الدخول في المسابقات والمنافسات، هي: "تضحية طوعية"، حيث إن البيانات الشخصية التي يتم الكشف عنها طوعاً قد تتعرض لاحقاً للسرقة أو تُستخدم لأهداف غير التي جُمِعت لها، كجرائم سرقة الهوية.[3]

(Identity Theft) - Identity theft is a form of stealing

---

(1) Robert R. Schriver، You Cheated، You Lied: the Safe Harbor Agreement and Its Enforcement By the Federal Trade Commission، 70 Fordham (2002) p 13

(2) https://coeia.ksu.edu.sa Accessed 20/3/2013 p.15

(3) Posner، R. A،The economics of privacy. The American Economic Review، 71(2)،. (1981). P405 - 409

someone's identity in which someone pretends to be someone else by assuming that person's identity، usually as a method to gain access to resources or obtain credit and other benefits in that person's name The victim of identity theft (here meaning the person whose identity has been assumed by the identity thief) can suffer adverse consequences if they are held responsible for the perpetrator's actions. Identity theft occurs when someone uses another's personally identifying information، like their name، identifying number، or credit card number، without their permission، to commit fraud or other crimes - .[(1)(2)]

ارتبط مفهوم الخصوصية بمصطلح حماية البيانات (Data Protection) مما جعلها تُضبط في إطار حماية البيانات الخاصة، نذكر من ضمن هذه التعريفات:

وزارة الداخلية السعودية: عرفت البيانات الشخصية، في مذكرتها للمبادئ الأساسية لأمن المعلومات وخصوصيتها، كالتالي: "كل ما يتعلق بالحياة الخاصة للإنسان كهويته وجنسيته واتجاهاته وميوله ومعتقداته وتعاملاته المالية والبنكية، فهي أي معلومات ترتبط بشخص مُعرَّف أو قابل للتعريف".[(3)]

---

(1) Hoofnagle، Chris Jay، Identity Theft: Making the Known Unknowns Known". Harvard Journal of Law and Technology"، Vol. 21، (2007) p.101

(2) سرقة الهوية هي قيام شخص بانتحال شخصية أخر، وغالبا ما يتم ذلك للاستيلاء على الحسابات البنكية والحصول على مزايا ائتمانية بصفة الشخص المعتدى عليه، ويتعرض الأخير جراء ذلك إلى مخاطر عديدة فيتحمل تبعات التصرفات الائتمانية التي ارتكبها المعتدي.

(3) فهد عبد العزيز سعود، مفهوم الخصوصية وتاريخها.. رؤية تقنية وإسلامية. مركز التميز =

- **ألـن ويسـتين (بروفسـور القانـون العـام):** "الخصوصيـة هـي حـق الأفـراد أو الجماعـات في أن يقـرروا بأنفسـهم زمـن ومـدى وكيفيـة مشـاركة المعلومـات الشـخصية مـع الآخريـن، وإذا نظرنـا إلى الخصوصيـة من مبـدأ المشـاركة الاجتماعيـة، فعندئذٍ تُعرف الخصوصيـة بأنهـا قـدرة الفـرد عـلى الانسـحاب الطوعي والمؤقت مـن المجتمـع العام عبر وسـائل مادية أو نفسـية".[1]

- **مكتـب خـبراء البيـت الأبيـض للعلـوم والتقنيـة:** "حـق الفـرد في الخصوصيـة هـو حقـه عـلى الاختيـار الشـخصي فيـما يريـد مقاسـمته مع الآخريـن مـن أفـكاره وعواطفـه والحقائـق المتعلقـة بحياتـه الشـخصية". [2]

و أيضـا عرفـت الخصوصيـة بأنهـا قـدرة الفـرد أو الجماعـة عـلى عـزل أنفسـهم أو معلومـات تخصهـم عـن الآخريـن، ثـم الرجـوع إلى الاجتماعيـة بصـورة انتقائيـة.

ومن أشـهر تعريفات الخصوصية:

التعريـف الـذي وضعـه معهـد القانـون الأمريـكي والـذي يتمتـع بقيمـة مهمـة في الولايـات المتحـدة، وهـو يعـرف الخصوصيـة عـن طريـق تعريـف المسـاس بهـا. فـكل شـخص ينتهـك حـق شـخص أخـر في ألا تتصـل أمـوره وأحوالـه إلى علـم الغـير وألا تكـون صورتـه عرضـه لأنظـار الجمهـور ويعتـبر مـن يفعـل ذلـك مسـؤولا أمـام المعتـدى عليـه.

وجـاء في التعليـق عـلى هـذا التعريـف أن التفرقـة بـين مـا يجـب إعلانـه للنـاس

= لأمن المعلومات 2012 ص 2.

(1) Bracy، Jedidiah. "Westin's Privacy Scholarship، Research Influenced a Generation GR.trnd 2013 P 4 See also Sullivan، Ronald. "Westin in Teaneck: Guiding a Magazine"، The New York Times، 1976.

(2) Jensen، Carlos Privacy policies as decision - making tools: an evaluation of online privacy notices(2004). P 98 See also. Privacy (Stanford Encyclopedia of Philosophy)". Plato.stanford.edu. Retrieved 2014 - 01 - 01.

وبين ما يجب أن يظل خفيا عنهم مازال من الأمور الدقيقة التي يصعب وجود معيار حاسم وواضح لها [1]

من الصعب وضع تعريف جامع مانع للحق في الحياة الخاصة، أو الحق في الخصوصية، لأن تعريف هذا الحق يرتبط بالتقاليد والثقافة والقيم الدينية السائدة والنظام السياسي في كل مجتمع.

فضلاً عن ذلك فإن أغلب التشريعات اتجهت إلى عدم إيراد تعريف للحق في الخصوصية، واكتفت بوضع نصوص تكفل حماية الحق وتعدد صور الاعتداء عليهِ.

ومن خلال ما تقدم يمكن أن نعرف الحق في الخصوصية بأنه: حق الأفراد في الحماية من التدخل في شؤونهم وشؤون عائلاتهم بوسائل مادية مباشرة، أو عن طريق نشر المعلومات عنهم.[2]

---

(1) دكتور حسام الدين الأهواني، الحق في احترام الحياة الخاصة، الناشر دار النهضة العربية،(1978(ص120

(2) عادل شمران الشمري، الانتهاك الإلكتروني لخصوصية الأفراد ووسائل مواجهتهُ،كلية القانون - جامعة كربلاء،)2010(ص87.

المطلب الرابع

صور الخصوصية وموقع خصوصية المعلومات بينها

يمكن في ضوء الاستعراض المتقدم تقسيم الخصوصية إلى عدد من الصور الذي لا يمنع الانفصال بينها وجود الارتباط الذي يجمعها جميعا في نطاق حق واحد هو حق الخصوصية، وهذه الصور هي:

أولاً: الخصوصية المادية:

وتشمل كل غرض مادي يعتبره الشخص سري ولا يمكن إطلاع الغير عليه، ويُشكل الجسد أحد هذه الأنواع، فقد كان الحبيب -صلوات الله وسلامه عليه - يختلي بنفسه في أول البعثة المكية في غار حراء، بعيداً عن أهل مكة وضوضائها، عابداً ربه قانتاً له. لم تُخترع الخزانات إلا لهذا النوع من الخصوصية، فتُخفى فيها الأموال والوثائق أو المقتنيات الشخصية أو المهمة، وكذلك الأقفال والأبواب.

والخصوصية الجسدية أو المادية Bodily Privacy هي التي تتعلق بالحماية الجسدية للأفراد ضد أية إجراءات ماسة بالنواحي المادية لأجسادهم كفحوص الجينات GENETIC TESTS، وفحص المخدرات DRUG TESTING. وتشمل بالطبع حماية جسد الفرد من أنشطة التفتيش وأنشطة الإيذاء غير القانونية.

و قد عرفت الخصوصية الجسدية بأنها:

Physical privacy could be defined as preventing "intrusions into one's physical space or solitude."[1]

(1) يمكن تعريف الخصوصية الجسدية بأنها الحق في عدم تعرض جسد الشخص للاعتداء والحفاظ على وجود مساحة آمنة محيطة.

This would include such concerns as:preventing intimate acts or hiding one's body from others for the purpose of modesty; apart from being dressed this can be achieved by walls، fences، privacy screens، cathedral glass، partitions between urinals، by being far away from others، on a bed by a bed sheet or a blanket، when changing clothes by a towel، etc.; to what extent these measures also prevent acts being heard varies

video، of aptly named graphic، or intimate، acts، behaviors or body parts

preventing unwelcome searching of one's personal possessions

preventing unauthorized access to one's home or vehicle(1)

ثانياً: الخصوصية المعلوماتية:

وهـي تشـير عـادةً إلى العلاقـة المُتضَمَنـة بـين التقنيـة والحـق الشرعـي في الخصوصيـة، مـن خـلال عمليتـي تجميـع المعلومـات الشـخصية ومشـاركتها.

وقـد يـرى البعـض عـدم مشـاركة أنـواع مختلفـة مـن البيانـات الشـخصية مـع الغـير مثـل: الديانـة والانتسـاب السـياسي والمعلومـات الصحيـة والأنشـطة

(1) H. Jeff،Managing Privacy: Information Technology and Corporate America Bookrule،USA، 2001 P 67 See also Security Recommendations For Stalking Victims". Privacyrights.org. Retrieved 2012 - 01 - 01. And "FindLaw›s Writ - Amar: Executive Privilege". Writ.corporate.findlaw.com. 2004 - 04 - 16. Retrieved 2012 - 01 - 01.

الخاصة، وذلك لأسباب عدة مثل: الإحراج الشخصي أو لتجنب المعاملة العنصرية أو العرقية أو التسبب بتعطيل السمعة المهنية له أو لغيره.

و تتضمن خصوصية المعلومات Information Privacy قواعد تحكم جمع وإدارة البيانات الخاصة كمعلومات بطاقات الهوية والمعلومات المالية والسجلات الطبية والسجلات الحكومية وهي المعبر عنها عادة باصطلاح حماية البيانات.[1]

ثالثاً: الخصوصية التنظيمية:

وتُعنى بحماية المعلومات ذات الحساسية عن المنشأة وأنشطتها، بالإضافة إلى البيانات الشخصية عن العاملين فيها. والمقصود بالمنشأة هنا، هي أي: "مجموعة من الأشخاص اجتمعوا ضمن قوانين وقيم محددة، ليحققوا هدف أو مجموعة من الأهداف المشتركة، ونجد أن المؤسسات والمنظمات تقوم بحفظ سرية (خصوصية) مخططاتها الإستراتيجية عن المنافسين لها، وكذلك أيضاً المنظمات الحكومية التي تقوم بحماية خصوصية البيانات الشخصية للمواطنين.[2]

والآن، ونحن نعيش في عالم تحيط بنا التكنولوجيا في جميع ممارساتنا اليومية، في حياتنا الخاصة وفي إدارة أعمالنا، أصبحت الخصوصية أحد الأمور التي تسعى كبار شركات التقنية وأمن المعلومات إلى حمايتها.

كما أن تقدم مجتمع المعلومات واعتراف الأفراد بأهمية السيطرة على المعلومات الشخصية الخاصة والتشديد على حماية أقوى البيانات الشخصية.

---

(1) Solove، Daniel J.، Rotenberg، Marc، Schwartz، Paul M. Privacy، Information، and Technology، Aspen Publ. (2006) pp. 9 - 11 See also Quinn، Michael J. Ethics for the Information Age،Sun Press، (2009).

(2) Bermann، S.،Information Privacy، Official Reference for the Certified Information privacy Professional (CIPP)، Swire(2007) p 12 See also Rechar،A،R Organization and it›s privacy، Stock Books، 1987

ومع ذلك، فإنه في الواقع من الصعب جدا على أي شخص السيطرة على المعلومات عن أنفسهم اليوم، بالإضافة إلى الكم الهائل من البيانات الشخصية، بما في ذلك المعلومات الشخصية والذي يجري جمعها وتخزينها على شكل رقمي في قواعد البيانات الخاصة والعامة.

ويساهم في عدم القدرة على السيطرة على تدفق البيانات الشخصية سهولة نقل البيانات الرقمية بالإضافة إلى أنه يمكن نسخها.

وفي الدول المتقدمة غالبا ما يكون الشخص على دراية بحقوقه الشخصية، وبالرغم من إقرار قوانين الخصوصية في عديد من الدول المتقدمة فإن الفهم الصحيح واستيعاب مبدأ الخصوصية والبيانات الشخصية لا يزال غامضا في بعض المجتمعات، وفي هذا الشأن تحديدا تلعب ثقافة المجتمع وأخلاقياته دورا كبيرا، فمجتمع مثل المجتمع الياباني لم يقر فيه قانون خاص بحماية البيانات الشخصية إلا في عام 2005 وذلك مواكبة لمتطلبات المجتمع الدولي مما جعل الالتزام باحترام قواعد الخصوصية وعدم التعدي على البيانات الشخصية تحديا يواجهه هذا المجتمع بالرغم من تطوره[1].

ونظرا للتطور التكنولوجي المتلاحق، وعدم قدرة القاعدة القانونية على مواكبة هذا التطور من حيث التقنين والتشريع - في ذلك فإن شأن البيانات الشخصية شأن كثير من المواضيع التي يطرأ عليها التطوير وغيرها من الموضوعات المستحدثة - نجد أن معظم التشريعات التي تتناول مواضيع الخصوصية بصفة عامة والقوانين التي تفرض حماية على البيانات الشخصية بصفه خاصة قليله نوعيا إن وجدت.

بصفة عامة يفرض القانون حماية البيانات الشخصية من خلال قوانين الخصوصية إلا أنه نظرا لأهمية حقل حماية البيانات الشخصية فقد فرض المشرع قوانين خاصة لحماية البيانات الشخصية.

---

(1) Yohko Orito and Kiyoshi Murata، "Privacy Protection in Japan:Cultural Influence on the Universal Value"،(2006) p.30

و قد كفلت الدساتير والقوانين الحق في الخصوصية للأشخاص، ومن العوامل التي يقاس بها مدى تحضر المجتمعات احترام المجتمع لحقوق الإنسان، ومن أبرز تلك الحقوق الحق في الخصوصية وحماية البيانات الشخصية، ومثال ذلك الدستور الأمريكي في تعديله الرابع عشر الذي أقر الحق في الخصوصية وحمايتها[1]، وكذلك مثل ما ورد في الإعلان البريطاني لحقوق الإنسان اعترافاً بالخصوصية.[2]

ولقد أصبحت حماية البيانات الشخصية محط اهتمام عالمي وليس على المستوى المحلي فقط نظرا لما نواكبه من تطور تكنولوجي متلاحق نظرا لسهوله تدفقها ونقلها.

و قد يطلق البعض على مفهوم البيانات الشخصية: معلومات شخصية أو معلومات التعريف الشخصي والتي تشير إلى المعلومات التي من الممكن أن تستخدم من أجل أن تعرف بشكل متفرد شخص ما أو مكان تواجده أو التي من الممكن استخدامها بالإضافة إلى مصادر أخرى لتعريف شخص ما بعينه.

على الرغم من قدم مصطلح معلومات شخصية بحد ذاته، فإنه أصبح ذا أهمية زائدة مع ظهور تقنيات المعلومات والإنترنت حيث أصبح تجميع وتنظيم المعلومات الشخصية أمرا أسهل نسبيا.

قد تستخدم المعلومات الشخصية من قبل المجرمين أو المحتالين من أجل التخطيط لجريمة قتل أو سرقة أو احتيال بحق شخص ما. كرد على مثل

(1) Mason، Alpheus Thomas Brandeis: A Free Man›s Life، Viking Press، (1946)، p. 70 See also."Right to Privacy Law & Legal Definition"، US Legal. Retrieved 17 October 2013.

(2) Gallop، Nick in The Constitution and Constitutional Reform (Philip Allan، 2011)، p.60

تلـك الاسـتخدامات الخاطئـة للمعلومـات الشـخصية فـإن العديـد مـن الـشركات ومواقـع الإنترنـت التـي تتعامـل مـع معلومـات شـخصية لشريحـة مـن الزبائـن يكـون لديهـا سياسـات خاصـة تتعلـق بحمايـة البيانـات الشـخصية للمسـتخدمين.

وسـوف يتـم تناول مفهوم البيانات الشـخصية بالتفصيـل في المبحث التالي.

المبحث الثاني

مفهوم البيانات الشخصية

إن الحاجة إلى تشريعات منفردة للبيانات الشخصية تتزايد يوما بعد الأخر، وفي ظل العالم التكنولوجي الذي نعيش بداخله أصبحت حماية المعلومات والبيانات الشخصية ذات أهمية قصوى، فقد تستغل هذه البيانات في كثير من الأغراض التي قد تضر بالحياة الاقتصادية والأمنية للمجتمعات.

- لذا تعين البحث في تعريف البيانات الشخصية (**المطلب الأول**).
- وكذلك أنواع البيانات الشخصية (**المطلب الثاني**).
- ثم تطور البيانات الشخصية من الناحية القانونية والتقنية (**المطلب الثالث**).

المطلب الأول

تعريف البيانات الشخصية

أصبحت حماية البيانات الشخصية موضوع خلاف في العالم الرقمي، خصوصا مع مشاركة الكثير من الأفراد مسائلهم الخاصة عبر الشبكات الاجتماعية.

إلا أنه يمكن التحكم في هذا الجانب من خلال اختيار عدم مشاركة تفاصيل محددة مع الآخرين، ولكن الجانب الآخر هو تطفل الشركات المزودة لخدمات الإنترنت على نمط الاستخدام لبعض أو جميع المشتركين، ومشاركة النتائج مع أطراف أخرى.

فمن الناحية الاجتماعية تزايدت أشكال شبكات التواصل الاجتماعي والتي تعتبر أحد أخطر المصادر التي تهدد خصوصية الأشخاص، فمثل هذه الشبكات ما هي إلا خزينة ضخمه للبيانات الشخصية للأشخاص وقد تؤدي قله الدراية القانونية للأشخاص إلى استغلال مقدمي الخدمات عن طريق شبكة الإنترنت وعن طريق برامج التليفون المحمول للبيانات الشخصية لهم.

وقد قضت محكمة أوروبا العليا على شركة جوجل العالمية بمحو بعض البيانات الشخصية الحساسة من ذاكرة المواقع والبحث، وأقرت أن للأشخاص الحق في عدم تتبعهم بواسطة الآخرين وذلك بعد تقديم شكوى من أحد المواطنين في إسبانيا حيث عرض محرك البحث جوجل بيانات تخص مسكن كان يود بيعه عن طريق نشر إعلان في الجريدة مما جعله يستاء من حفظ مثل هذه البيانات.[1]

---

(1) Court of Justice of the European Union، PRESS RELEASE No 70/14، Luxembourg، 13 May 2014، Judgment in Case C - 131/12، Google Spain SL، Google Inc. v Agencia Española de Protección de Datos، Mario Costeja González

وقد وضع الحكم حدا فاصلا للخلاف بين المدافعين عن خصوصية المعلومات والبيانات الشخصية وأولئك المدافعين عن الحق في حرية التعبير.

وقد تضمن الحكم أيضاً إلزام شركة جوجل العالمية بمحو وتعديل الروابط التي تحتوى على بيانات شخصية قديمة وغير محدثة، وقد أضاف القاضي في حكمه أن محرك البحث يعد مسؤولا عن معالجة البيانات الشخصية والتي يتم استغلالها من شخص أخر.

وقد أضاف Marc Rotenberg [1] إن مثل هذا الحكم يعد تدعيما لمبدأ حماية خصوصية البيانات الشخصية عبر الإنترنت، وأضاف إن مثل هذا الحكم سوف يضيف قيود تنظيمية على مثل هذه الشركات.

وقد أضاف الحكم إن حماية البيانات الشخصية للأفراد تعلو على المصلحة الاقتصادية للشركات.

ومن وجهة النظر الأمريكية لا تعد محركات البحث مسؤولة عن محتوى محرك البحث، حيث لا تعد الشركة مقدمة الخدمة مسؤولة عن معالجتها أو الاستيلاء عليها بواسطة طرف ثالث.[2]

وكذلك فإن بعض مغريات التواصل الاجتماعي تجعل الأشخاص يفصحون عن بياناتهم الشخصية طواعية مما قد يسبب لهم الكثير من المشاكل القانونية ولكن مثل الحكم السابق قد يضع حداً لاستغلال البيانات الشخصية مع أن ذلك من الناحية العملية فمثلا برامج مثل Viber، What'sapp[3] تتيح لمقدم الخدمة الدخول على سجل الهاتف والاستحواذ على نسخه البيانات وأرقام الهواتف المسجلة وهذا لا يعد فقط تعديا على البيانات الشخصية

(1) Marc Rotenberg، executive director of the Electronic Privacy Information Center in Washington، D.C

(2) Joel Reidenberg، information law and privacy، a U.S. Says 2014 p 39

(3) برامج متوفرة لأجهزه التليفون الحديثة للتواصل عن طريق الرسائل النصية.

للمستخدم فقط بل وغيرهم من يمتلك هو جزء من بياناتهم الشخصية بهدف التواصل معهم.[1]

ومن الناحية الاقتصادية أصبحت البيانات الشخصية للأفراد جزءا لا يتجزأ من رأس مال الشركات حيث تقوم شركات متخصصة في إعداد قواعد البيانات وتصنيفها ببيع هذه القواعد والتي تحتوي على بيانات شخصية لآلاف العملاء وتستخدم هذه البيانات بعده طرق إما بالاستهداف المباشر للعميل عن طريق الاتصال أو إرسال الإعلانات الدعائية والترويجية للسلع، أو تستخدمها الشركات بهدف دراسة السوق ومتطلباته، كذلك القيام بالتصنيف العمري والتعليمي وغيره.[2]

وقبل البحث في كيفية حماية البيانات الشخصية يجب أولا تعريف البيانات الشخصية:

فبداية هي البيانات التي يمكن من خلالها تعريف الشخص الطبيعي وكذلك الاعتباري معروفا أو قابل للتعريف للأخر.

ويمكن أيضا تعريف البيانات الشخصية بأنها: " أي معلومات تتعلق بشخص طبيعي محدد أو يمكن تحديده "موضوع البيانات"، بشكل مباشر أو غير مباشر".[3]

وفي هذا التعريف يتم الإشارة إلى أن البيان في حد ذاته دون جدوى إلا لو التصق بشخص معين، فمثلا الرقم القومي للشخص في حد ذاته لا يعبر عن شيء بعينه إلا إذا نسب إلى صاحب البطاقة.

---

(1) Shade، L. R. Reconsidering the right to privacy in Canada. Bulletin of Science، Technology & Society، (2008).P 80 - 91

(2) http://icsa.cs.up.ac.za/issa/2004/Proceedings/Full/078.pdf. Accessed 16 July(2012) p.43

(3) Narayanan، A.; Shmatikov، V. (2009). "De - anonymizing Social Networks". 2009 30th IEEE Symposium on Security and Privacy. p. 173

ومن المفترض أن يكون تعريف البيانات الشخصية واسع جدا حيث تكون المعلومة بيانا شخصيا البيانات الشخصية عندما يقوم شخص ما قادر على ربط المعلومات لشخص.

ومن ثم فإن ارتباط المعلومة بالشخص يجعلها من البيانات الشخصية على سبيل المثال: عنوان السكن إذ أن عنوان السكن بمعزل عن الشخص الذي يقطن المكان لا يعد بيانا شخصيا ومن ثم ارتباطه بالشخص هو الذي يجعل منه بيانا شخصيا.

في حين أن بعض البيانات التي تتعلق بالضرورة للفرد من تلقاء نفسها، مثل اسم الفرد.

وفي الولايات المتحدة الأمريكية يطلق على البيانات الشخصية بيانات التعريف الشخصي PII[1]

معلومات التعريف الشخصية " (PII)، كما تستخدم في قانون الخصوصية وأمن المعلومات بالولايات المتحدة، هي المعلومات التي يمكن استخدامها بمفردها أو مع غيرها من المعلومات للتعرف على أو تحديد شخص واحد، أو لتحديد الفرد في سياق.[2]

المعلومات الشخصية " يشمل أيضا المعلومات التي تحدد هوية الشخص على الرغم من أن مفهوم PII مفهوم قديم فإنه قد أصبح أكثر أهمية مثل تكنولوجيا المعلومات وقد جعل التطور التكنولوجي جمع بيانات التعريف الشخصي من خلال خرق أمن الإنترنت، وأمن الشبكات وأمن متصفح الويب أمرا مربحا، مما يؤدي إلى سوق مربحة في جمع وإعادة بيع PII.

(1) John M.K PII: Personal Identifiable Information p، US press release 1999 p.56

(2) Vincent D. Blondel "Unique in the Crowd: The privacy bounds of human mobility". Nature srep2013، p 78

وتعـرف مذكـرة مكتـب الإدارة والميزانيـة بالبيـت الأبيـض -الولايـات المتحـدة - البيانـات الشـخصية عـلى النحـو التـالي:

المعلومـات التـي يمكـن اسـتخدامها لتمييـز أو تعقـب هويـة الفـرد، مثـل الاسـم ورقـم الضـمان الاجتماعـي، والسـجلات الحيويـة، الـخ وحدهـا، أو عنـد دمجهـا مـع المعلومـات الشـخصية أو تحديـد الأخـرى التـي ترتبـط أو للربـط إلى شـخص معـين، مثـل تاريـخ ومـكان الـولادة، واسـم عائلـة الأم، الـخ[1]

Information which can be used to distinguish or trace an individual's identity، such as their name، social security number، biometric records، etc. alone، or when combined with other personal or identifying information which is linked or linkable to a specific individual، such as date and place of birth، mother's maiden name، etc[2].

يتـم تعريـف مصطلح البيانات الشـخصية في توجيه الاتحاد الأوروبي:

البيانـات الشـخصية: تعنـي أي معلومـات تتعلق بشـخص طبيعـي محدد أو يمكن تحديـده (' موضـوع البيانـات ')؛ بشـخص معـروف واحـد هـو الـذي يمكـن تحديدهـا، بشـكل مباشر أو غـير مباشر، ولاسـيما من خلال الإشـارة إلى رقم هويـة أو لواحد أو أكثر مـن العوامـل المحـددة لهويتـه البدنيـة والفسـيولوجية والعقليـة والاقتصاديـة والثقافيـة والاجتماعية.

personal data' shall mean any information relating to

---

(1) http://www.whitehouse.gov/sites/default/files/omb/assets/legislative_reports/fy14_preview_and_joint_committee_reductions_reports_04102013.pdf retrived 12 - 3 - 2014

(2) Narayanan، A.; Shmatikov، V. "Myths and fallacies of "personally identifiable information"". Communications of the ACM53 (6) (2010). p.24.

an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified، directly or indirectly، in particular by reference to an identification number or to one or more factors specific to his physical، physiological، mental، economic، cultural or social identity.[1]

أما في أستراليا فقد عرف قانون الخصوصية لعام 1988 وذلك باستخدام مبادئ OECD[2] للخصوصية لعام البيانات الشخصية 1980 بأنها:[3]

تعني المعلومات أو الآراء (بما في ذلك معلومات أو رأي يشكل جزءا من قاعدة بيانات)، سواء كانت صحيحة أم لا، وسواء سجلت في شكل مادي أم لا، عن فرد هويته واضحة، أو يمكن التأكد بشكل معقول، من المعلومات أو الآراء.

Personal information" means information or an

(1) Stephen F. Laribee & Stephen D. Hogan، The Right to Privacy and Person Data: The EU Prods the U.S. and Controversy Continues، 9 Tulsa J. Comp. & Int›l L. (2002) P 391، 441

(2) Internationally، the OECD Privacy Principles provide the most commonly used privacy framework، they are reflected in existing and emerging privacy and data protection laws، and serve as the basis for the creation of leading practice privacy programs and additional principles.The OECD Privacy Principles tie closely to European Union (EU) member nations› data protection legislation (and cultural expectations)، which implement the European Commission (EC) Data Protection Directive (Directive 9546//EC)، and other "EU - style" national privacy legislation. (The European Commission is the executive body of the European Union.)

(3) "Asturalia Privacy Act 1988". Retrieved 14 - 10 - 2013.

opinion (including information or an opinion forming part of a database)، whether true or not، and whether recorded in a material form or not، about an individual whose identity is apparent، or can reasonably be ascertained، from the information or opinion.[1]

هـذا يثـير مسـألة منطقيـة: تفـترض أنـه مـن الممكـن نظريـا لتحديـد هويـة الشـخص مـن المعلومـات الأساسـية التـي لا تتضمـن اسـم وعنـوان بسـيط ولكـن تحتـوي عـلى القرائـن التـي يمكـن تتبعهـا للتأكـد مـن صلته بهـا فقـط، وبالتالي قـد أضاف المشرع الأسـترالي مجـالا أوسـع لتعريـف البيانـات الشـخصية مـن المـشرع الأمريـكي.

وفي تعريـف قانـون حمايـة البيانـات الشـخصية والمسـتندات الإلكترونيـة الكنـدي ورد تعريـف البيانـات الشـخصية بأنهـا: هـي المعلومـات الخاصـة بشـخص معـرف ولكـن لا تشـمل الاسـم، الوظيفـة، عنـوان وتليفـون العمـل لموظـف يعمـل بإحدى الـشركات.[2]

Personal Information Protection and Electronic Documents Act (2000، c. 5) (PIPEDA) states that "personal information" means "information about an identifiable individual، but does not include the name، title or business

---

(1) Raymond Wacks، Privacy: A Very Short Introduction، Oxford: Oxford University Press، 2009 P 67

(2) McClennan، Jennifer P.; Schick، Vadim (2007). "O، Privacy: Canada›s Importance in the Development of the International Data Privacy Regime". Georgetown Journal of International Law 38: 669–693 see also PIPEDA Review – Privacy Commissioner of Canada http://web.archive.org/web/20100813133308/http://www.priv.gc.ca/keyIssues/ki - qc/mc - ki - pipeda_e.cfm retrived 23 - 7 - 2012

address or telephone number of an employee of an organization."[1]

وبالرغـم مـن أن الاسـم والوظيفـة وعنـوان وتليفـون العمل مسـتثنى مـن تعريف البيانـات الشـخصية وكذلـك الحمايـة القانونيـة للبيانـات الشـخصية وفقـا قانـون حمايـة البيانـات الشـخصية والمسـتندات الإلكترونيـة الكنـدي فـإن البريـد الإلكـتروني الخـاص بالعمـل مشـمول بالحمايـة ويعتـبر مـن البيانـات الشـخصية.[2]

وقـد لوحـظ في التعاريـف المختلفـة أن المعلومـات أو البيانـات لا تكـون شـخصية إلا لكونهـا ملتصقـة بشـخص بعينـه فالاسـتيلاء عـلى البيـان لا يمثـل خرقـا في حـد ذاته إلا لـو كان ملتصقـا بشـخص.

ومـن الملاحـظ أيضـا أن اسـتخدام مصطلـح الشـخص المعـرف أو القابـل للتعريـف ينطـوي عـلى اسـتخدام تلـك المعلومـات والبيانـات في تعريـف الشـخص سـواء أكانـت منفـردة أم مدمجـة مـع بيانـات أخـرى.

وفي توضيـح أخـر أقـر عـدم ضرورة توثيـق البيانـات حتـى يطلـق عليهـا بيانـات شـخصية أو تشـمل بالحمايـة القانونيـة وتكفـي لضـمان هـذه الحماية أن تكـون البيانات ملتصقـة بشـخص بعينـه، ومـن أمثلـه ذلـك المحادثـات الشـفوية وعينـات التحاليـل الطبيـة التـي تسـحب مـن جسـم الإنسـان فقـد تتغـير نتائـج هـذه التحاليـل مـن مرة إلى أخـرى، ومـن هنـا فهـي معلومـات غـير موثقـة، ولكنهـا تعـد بيانـات شـخصية والاعتـداء عليهـا بالاسـتيلاء أو النـشر أو غـيره يدخـل تحـت مظلـه حمايـة البيانـات الشـخصية[3].

---

(1) Section 2(1) of the "Personal Information Protection and Electronic Documents Act " (2000، c. 5) p.34

(2) PIPEDA Case #2005 - 297 - Unsolicited e - mail for marketing purpose.available https://www.priv.gc.ca/leg_c/interpretations_02_e.asp p.100

(3) Morgan v. Alta Flights Inc. (2006) FCA 121، affirming (2005) FC 421 case in privacy law.available at https://www.priv.gc.ca/leg_c/interpretations_02_e.asp p.43

ولا يعني اشتراك أكثر من شخص في بيان شخصي واحد أو معلومة أنها تخرج من دائرة تعريف البيانات الشخصية، ولكنها تصنف أيضا بيانا شخصيا يشمل بالحماية القانونية للبيانات الشخصية، فمثلا المحادثات والآراء التي يدلي بها شخص للمدح أو للذم في شخص آخر تعد بيانات شخصية لكلا منهما، وكذلك عنوان السكن للمنزل الذي تقطنه أسرة يعتبر بيانا شخصيا مشتركا لهم جميعا، وكذلك تليفون العمل الذي يستخدمه أكثر من موظف.(1)

وتظل أيضا المعلومات مصنفة بأنها بيانات شخصية حتى وإن أصبحت متاحة للعامة عن طريق التنازل طواعية من الشخص صاحب البيان، مثال ذلك عند ملء الاستمارات للحصول على خدمة أو وظيفة فهنا يتنازل الشخص عن مجموعة من البيانات الشخصية نظير تلقيه الخدمة، وهنا من حق مقدم الخدمة استغلال هذه البيانات بالبحث أو التسجيل، ولكن هذا مشروط فقط بحدود الخدمة المقدمة وهذا لا يعتبر تعديا على البيانات الشخصية، ومن جانب آخر لا يعد هذا التنازل بمثابة نزع الصف أو الحماية عن البيانات الشخصية المفصح عنها.

وتعتبر البيانات بيانات شخصية حتى وإن لم تكن دقيقة أو غير صحيحة وقد عرفت لجنة حماية البيانات الشخصية في سنغافورا البيانات الشخصية بأنها:

البيانات كانت صحيحة أو غير صحيحة التي تعبر عن الشخص القابل للتعريف وذلك عن طريق البيانات أو عن طريق البيانات وغيرها من المعلومات المتوفرة لدى الشركة أو تستطيع الحصول عليها.(2)

---

(1) Sawer، Patrick، "Police use glove prints to catch criminals". Telegraph.co.uk. Retrieved 2013 - 08 - 20. (2008 - 12 - 13). P.24

(2) Bright، Peter "Doxed: how Sabu was outed by former Anons long before his arrest". Ars Technica. (2012).

Personal data is Personal data is defined in the PDPA as “data، whether true or not، about an individual who can be identified

1. from that data; or

2. from that data and other information to which the organization has or is likely to have access. is likely to have access.[1]

و بالتالي فمفهوم البيانات الشخصية ينطبق على البيانات التي تعرف الشخص سواء كانت هذه البيانات صحيحة أم غير صحيحة، فتحديد كون المعلومة أو البيان بيانا شخصيا أم لا، لا يرتبط بصحة البيان من عدمه ولكن بكونه لصيق بالشخص صاحب البيان.

وبالارتباط البيانات والمعلومات ببعض مناحي الحياة يمكن تحديد ما إذا كانت ضمن سياق البيانات الشخصية أو لا.

أولا: في سياق الشركات والموظفين عامة ما تكون المعلومات الخاصة بالشركات:

لا تعد بيانات شخصية في حد ذاتها إلا إذا اتصلت بشخص بعينه، مثلا ارتباط بيانات صاحب الشركة بالشركة هنا تظل البيانات الشخصية لصاحب الشركة متمتعة بالحماية للبيانات الشخصية، وغير ذلك فتعد الرسائل والبريد الإلكتروني والعمليات التي يجريها الموظف داخل الشركة وغيرها من الخدمات التي يعتبر أداؤه أو آراؤه جزء لا يتجزأ منها وكذلك أرقام لحسابات والرموز السرية وغيرها من البيانات المرتبطة بالشخص

(1) ADVISORY GUIDELINES ON KEY CONCEPTS IN THE PERSONAL DATA،PROTECTION ACT،ISSUED BY THE PERSONAL DATA PROTECTION COMMISSION،(24 SEPTEMBER 2013) p.51

داخـل مـكان عملـه مـن البيانـات الشـخصية وبالقيـاس عـلى ذلـك فالشـكاوى المقدمـة ضـد الموظـف تكـون ضمـن البيانـات الشـخصية إذ تتضمـن أراء شـخص أخر فيـه ويجب أن تشـمل بالحمايـة.[1]

وبالتـالي فـإن التقييـم الـدوري لأداء الموظفـين كذلـك التقاريـر التـي يكتبهـا المديـرون تعـد مـن البيانـات الشـخصية للموظفـين.

ثانيا: في سياق صحة الشخص وتاريخه العلاجي:

تعـد التقاريـر الطبيـة والعينـات التحليليـة مـن البيانـات الشـخصية للشـخص وتدخـل ضمـن تعريـف البيانـات الشـخصية وتشـمل بالحمايـة القانونيـة، وكذلـك تعتـبر التقاريـر الطبيـة مـن البيانـات الشـخصية للطبيـب في الوقـت ذاتـه حيـث إنـه يعـبر فيـه عـن رأيـه في شـخص آخـر وبالتـالي التعـدي عـلى التقاريـر الطبيـة يعـد انتهـاكا للبيانـات الشـخصية للطبيـب أيضـا.

لكـن في حالـه إجـراء فحـص لإعـداد تقاريـر طبيـة لتقديمهـا للجهـات بعينهـا وبالرغـم مـن أنهـا تشـمل بيانـات شـخصية فإنهـا لا تمثـل تعديـا عـلى البيانـات الشـخصية لتقديمهـا طواعيـة مـن صاحـب التقريـر.[2]

ومـن أمثلـه البيانـات الشـخصية التـي لهـا علاقـة بصحـة الشـخص: المعلومـات حـول حالتـه الصحيـة والعقليـة والتشـخيص المرضي وجرعـات الأدويـة والتقاريـر الدوريـة للأمـراض المزمنة.[3]

---

(1) Westin، A. Privacy and freedom (Fifth ed.). New York، U.S.A.: Atheneum (1968) p.120.

(2) PIPEDA Case Summary #2009 - 018 – Psychologist's anonym zed peer review notes are the personal information of the patient. P.130

(3) Marh John Trane، "Comments of Latanya Sweeney، Ph.D. on "Standards of Privacy of Individually Identifiable Health Information"". Carnegie Mellon University

ثالثا: في السياق المعاملات المالية:

البيانات المتعلقة لأموال الشخص واستثماراته تعد بيانات شخصية، فمثلا الحسابات البنكية ومعلومات القروض والاستثمارات تعد من ضمن البيانات الشخصية التي تتمتع بحماية قانونية.

وتعد الإشارة البسيطة للديون الشخصية حتى وإن لم تحتو على تفصيلات كافية تدخلا في الحياة الخاصة للفرد واعتداء على بياناته الشخصية.

وقد حكمت محكمة ولاية كاليفورنيا العليا في العاشر من فبراير 2011 بإدانة موظف البنك الذي تحرى عن الرقم البريدي بخصوص تعاملات تجري على البطاقة الائتمانية واعتبر الرقم البريدي من بيانات التعريف الشخصي والتي تشمل تحت مظلة حماية البيانات الشخصية.[1]

وتعتبر البيانات شخصية كل بيان يعرف ويساعد على تعريف الشخص سواء كان هذا البيان أو المعلومة في شكل مادي أو إلكتروني فلا يعتبر الوسيط الذي تقدم أو تستخدم من خلاله البيانات معيارا لتحديد ما إذا كانت المعلومة المتداولة بيانا شخصيا أم لا، فطالما تستخدم المعلومة للتعريف بالشخص أو تساعد في ذلك التعريف تعد بيانا شخصيا.

وتعتبر البيانات بيانات شخصية بغض النظر عن الوسيط أو المرجعية المستخدمة إما لتخزين أو استخدام مثل هذه البيانات قد تكون محتوى قاعدة بيانات مكتوبة أو كتاب أو وسيط إلكتروني سواء بالحفظ أو بالإرسال فيعد البيان شخصيا إذا ارتبط بشخص معين بغض النظر عن الوسيط المستخدم.[2]

---

(1) By Daniel T. Rockey،Requesting at Point of Sale Subject to Statutory Penalties،، Counsel، Bullivant Houser Bailey PC 2011. P 23

(2) M، Valcke. "T. Computers & Education". Elsevier Ltd.،2012. P73 See also Posner، R. A.. Privacy right. The American Economic Review، 1989

وقد أكدت التعريفات السابقة على أن الشخص يمتلك بياناته الشخصية وله حق التصرف فيها، إذ أنها تعبر عن شخصه وذاته وله الحق في استعمال تلك البيانات والتنازل المؤقت عنها ومنح حق الاستغلال للآخرين أيضا، ولكن امتلاك الشخص للبيان الشخصي لا يمنحه حق استغلال هذا البيان بمعزل عن كونه بيانا شخصيا، فمثلا العنوان يمتلك الشخص عنوان سكنه ولكن ليس لديه الحق في استغلال أو تغيير اسم الشارع.[1]

وأيضا إذا تم التقاط صورة للشخص في مؤسسة حكومية هنا تعد بيانا شخصيا ومملوكا لصاحب الصورة، ولكن ملكية الصورة كشيء ترجع للمؤسسة.

كذلك الاسم فليس مبررا أن شخصا ما يدعى أحمد أنه أمتلك الاسم ذاته وبإمكانه قصر هذا الاسم على نفسه أو إلغائه لكن ما يمتلكه هو اسمه الذي يعرفه هو بالإضافة إلى اسم عائلته.

وبالتالي يمتلك الشخص البيان الشخصي طالما استخدم في تعريفه ولكن ملكية الأشياء تظل لمالكها الأصلي بمنأى عن اتصال الشيء بالشخص صاحب البيان.

ومن خلال ما تقدم نخلص إلى أن البيانات الشخصية هي:

البيانات والمعلومات التي تتعلق بشخص طبيعي أو اعتباري محدد ومعروف أو قابل للتعريف عن طريق تلك البيانات والتي تستخدم لتميز الشخص عن غيره وتحديد هويته سواء كانت تلك البيانات دقيقه أم غير دقيقة، تعد في حد ذاتها بيانا أو تحتاج إلى معلومات إضافية للتوضيح سواء كانت في شكل مادي أم إلكتروني وكل بيان أو معلومة يعبر عن الحالة العقلية،

---

(1) Flaherty، D. "Protecting privacy in surveillance societies": The federal republic of Germany، Sweden، France، Canada، and the United States. Chapel Hill، U.S.: The University of North Carolina Press (1989) p.43

الصحيـة، الثقافيـة، الاجتماعيـة أو المهنيـة وكل مـا يرتبـط بالشـخص ومعاملاتـه وآرائه أو آراء الغـير فيـه تعـد بيانات شـخصية.

يمكـن تحديـد البيانـات الشـخصية المتعلقـة بالأفـراد مـن خـلال دراسـة عـده جوانـب وذلـك نظـرا لعـدم وجـود حـصر كامـل لأنـواع البيانـات الشـخصية للأفـراد.

المطلب الثاني

أنواع البيانات الشخصية

يمكن دراسة البيانات الشخصية من أكثر من زاوية وذلك مع التطور البشري، فلم تعد تلك البيانات مقصورة على الاسم والعنوان بل تطور المفهوم ليشمل:

- البيانات عبر وسيط شبكي **(الفرع الأول)**.
- وكذلك من الناحية أو المنظور الاجتماعي **(الفرع الثاني)**.
- وتعتبر البيانات الصحية للشخص بيانات شخصية **(الفرع الثالث)**.
- ويحتوى المنظور التعليمي والوظيفي والمالي على العديد من البيانات الشخصية **(الفرع الرابع)**.

الفرع الأول

من الناحية التكنولوجية

هي كل البيانات الشخصية التي يتم تداولها عن طريق استخدام وسيط إلكتروني، أو نشرها عبر شبكة الإنترنت والتي يمكن من خلالها تعريف الشخص[1].

وقد تم نقد هذا التعريف إذ أنه لم يوصف أو يحدد البيانات الشخصية في حد ذاتها ولكن فقط عرف الوسيط الذي يتم تداول تلك المعلومات والبيانات من خلاله، وبالتالي لا يصلح هذا التعريف لوضع نطاق للبيانات الشخصية المتعلقة بالأفراد وتميزها عن ما لا يعد بيانا شخصيا.[2]

كما أسلفنا فإن التطور التكنولوجي قد أعطى لمفهوم البيانات الشخصية عمقا جديدا، وقد يطلق عليها أيضا الخصوصية المعلوماتية، ومن ثم فجميع البيانات التي تتداول عبر الوسيط الشبكي وتكون متصلة بشخص بعينه يمكنها تعريفه منفردا أو عن طريق إضافتها لبيانات أخرى مثل الاسم والحسابات الإلكترونية من بريد إلكتروني أو حسابات على مواقع التواصل الاجتماعي بالإضافة إلى الأرقام السرية بالإضافة إلى الصور والأخبار والتعليقات والآراء.

وتجدر الإشارة هنا إلى أن البيان يعد في حد ذاته يعد بيانا شخصيا

---

(1) Paul M. Schwartz & Daniel J. Solove، "The PII Problem: Privacy and a New Concept of Personally Identifiable Information"، 86 N.Y.U. L.REV. 1814 (2011)، available at http://ssrn.com/abstract1909366 p.11

(2) Popa، C..، "Managing Personal Information: Insights on Corporate Risk and Opportunity for Privacy - Savvy Leaders"، Carswell (2012) p.17 See also John M،Privacy Rights Clearinghouse، a consumer education and privacy rights advocacy organization،2010

وبـدون توثيـق طالما ارتبطـت بشـخص معـرف أو قابـل للتعريـف، هـذا بالإضافـة إلى أن الوثائـق التـي تثبـت تلـك البيانـات تعـد بيانـات شـخصية أيضـا، وعـلى ذلـك فـكل شيء يرتبـط بالأشـخاص مـن حيـث تعريفهـم يعـد بيانـا شـخصيا.[1]

وقـد ذهـب البعـض لتحديـد نطـاق البيانـات الشـخصية المتعلقـة بالأفـراد عـن طريـق تميزهـا عـن البيانـات العامـة وقـد عـرف هـذا الاتجـاه البيانـات الشـخصية بأنهـا البيانـات غـير العامـة أو التـي لا تتعلـق بالشـخص حيـث أضـاف أن كل بيان شـخصي هو ذلـك البيـان الـذي لا يدخـل في نطاق الإطـار العام بعيدا عـن تعريف البيانات الشـخصية بأنهـا تلـك التـي تسـتخدم في تعريـف الشـخص، فقد حـدد البيانـات الشـخصية بأنها تلك البيانـات غـير المنشـورة التـي لا يمكـن الوصـول إليهـا، وغـير المتاحـة في السـجلات العامة وبالتـالي وفقـا لهـذا المبـدأ لا يعـد الاسـم والعنـوان وغيرهـا مـن البيانـات التـي توجـد في السـجلات الحكوميـة بيانـات خاصـة وقـد اسـتدل هـذا المبـدأ بتعريـف القانـون الألمـاني The Gramm - Leach - Bliley Act (GLBA)، البيانـات الماليـة للشـخص عـلى أنهـا البيانـات غـير العامـة، ومـن هنـا تعـد مثـل هـذه البيانـات بيانات شـخصية.[2]

وأيضـا يتناقـض مـع المبـدأ السـابق حيـث إن في مضمـون تعريفـه أنهـا البيانـات المنشـورة عـلى الإنترنـت وهنـا وبالنسـبة للمبـدأ السـابق يدخل تحـت طائلـة القانون كل مـن يسـتغل البيانـات أمـا بالنسـبة لهـذا المبـدأ يدخـل تحـت طائلـة القانـون ليـس فقط كل مـن يسـتغل تلـك البيانـات ولكنهـا يمكـن أن تنتهـك بالإطـلاع.

---

(1) Larose، R.، & Rifon، N. J. Promoting i - Safety: Effects of Privacy Warnings and Privacy Seals on Risk Assessment and Online Privacy Behavior. Journal Of Consumer Affairs، (2007). 127–149.

(2) Martin Hilbert and Priscila López،"The World's Technological Capacity to Store، Communicate، and Compute Information"، especially Supporting online material، Science (journal)، (2011).P 65

الفرع الثاني

من الناحية الاجتماعية

بداية تعد البيانات الشخصية من المنظور الاجتماعي هي أساس دراسة البيانات الشخصية وتتمثل في عدة بيانات مثل:

1. الاسم:

وهو الوسيلة التي يتميز بها الشخص عن غيره. وللاسم معنيان معنى ضيق ويقصد به الاسم الشخصي، والمعنى الثاني يقصد به اللقب أو اسم الأسرة.

وهناك أنواع أخرى للاسم يحميها القانون إذا استعملت بصفة مستمرة وحمايتها تكون بقدر حماية الاسم المدني من ذلك اسم الشهرة والاسم المستعار والاسم التجاري.

اسم الشهرة: وهو اشتهار الشخص باسم آخر بين الناس واسم الشهرة هو من صنع الناس أي الغير هو الذي يطلق على الشخص هذا الاسم واسم الشهرة جدير بحماية القانون. [1]

الاسم المستعار: ويطلقه الشخص على نفسه بقصد معين كإخفاء شخصيته في مناسبة معينة وقد يكون الغرض سياسيا كتسمية رجال المقاومة بأسماء مستعارة لإخفاء أسمائهم الحقيقية والشخص حر في اختيار هذا الاسم وكذلك هذا الاسم يحميه القانون إذا استعمله صاحبه بصفة مستمرة.

---

(1) Muench، David "Wisconsin Community Slogans: Their Use and Local Impacts"، December 1993. Retrieved April 10، 2007.

الاسم التجاري: وهو استخدام التاجر اسما يمارس تحته تجارته ويكون مميزا لمحله التجاري، وعنصرا من عناصره وهو حق مالي قابل للتصرف فيه.

و يعد أيضا اسم الوالد والوالدة من البيانات الشخصية للفرد.[1]

2. الموطن:

هو المكان الذي يقطنه أو يستخدمه لإدارة نشاط معين للفرد وغالبا ما يتكون من رقم العقار واسم الشارع والمنطقة والمحافظة وفي هذا السياق يجب التفرقة بين العنوان والمحل القانوني، فالمحل القانوني هو ذلك العنوان الذي يختاره الشخص لتلقي المراسلات والمدرج في العقود التي يبرمها وقد يكون هذا العنوان عنوان السكن أو العمل أو حتى مكتب المحامي الذي يوكله الشخص.

3. السن أو تاريخ الميلاد وشهادة الميلاد.

4. أرقام التليفون.

5. الحالة الاجتماعية سواء كان: (متزوج، أعزب أو مطلق) وبالتالي الشهادات التي تثبت هذه الحالة.

6. أرقام بطاقات تعريف الهوية مثل بطاقات الرقم القومي وجواز السفر ورقم التأمين الاجتماعي.

7. الديانة.

---

(1) "Did LulzSec،Trick Police Into Arresting the Wrong Guy? - Technology". The Atlantic Wire. 2011 p - 28 See also "Directive 9546//EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data availble at wwww.eumpcouncil.org See also "Protection of personal data - Justice". Ec.europa.eu. 2011 - 01 - 18. Retrieved 2012 - 10 - 23.

8. الجنس أو النوع.

9. الانتماء السياسي لدولة معينة سواء الاتصال به بالدم أو بالميلاد. وكذلك الآراء ووجهات النظر سواء في مواضيع عامه أو شخص بعينه.

10. الصورة والفيديو الذي يظهر فيه الشخص.

11. المراسلات.

الفرع الثالث

من الناحية الصحية

تعرف البيانات الشخصية الصحية عن طريق برنامج حماية أبحاث الإنسان بأنها أي معلومات عن التاريخ الصحي للشخص أو تاريخ التشخيص والتي يمكن أن تستخدم لتعريف شخص بعينه، والتي قد استخدمت من قبل لتقديم خدمه طبية مثل التشخيص أو العلاج، بالإضافة إلى بيانات الحمض النووي للشخص وغيرها من التحاليل والفحوصات الطبية الخاصة بالشخص.[1]

---

(1) Narayanan، A.; Shmatikov، V. "Myths and fallacies of "personally identifiable information"". Communications،(2010). P 24.See alsoJames،N.J "Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)" thmases،2013See also Malcolm Clarke،Developing a Standard for Personal Health Devices based on 11073 (Conf Proc IEEE Eng Med Biol Soc. 2007) See also James W.H. McCord and Sandra L. McCord، Criminal Law and Procedure for the paralegal: a systems approach، supra، 2000 See also "De - identification". ucdmc.ucdavis.edu. 2011

الفرع الرابع

من الناحية المهنية والتعليمية والمالية

تعتبر البيانات التي ترتبط بالتاريخ الوظيفي للشخص بيانات شخصية كذلك المتعلقة بأدائه الوظيفي وكذلك رقم تعريفه في العمل، المرتبات، الاستحقاقات المادية والمعنوية، إجراءات الاختيار والتعين والمراقبة أثناء العمل من خلال المكاتب، التليفونات، والبريد الإلكتروني[1].

وكذلك تعتبر البيانات الشخصية التعليمية التي تحدد المستوى الدراسي للشخص والدرجات العلمية التي حصل عليها، وتعتبر الحسابات البنكية أو أرقام كروت الائتمان وبيانات القروض وتقارير الحسابات البنكية وكل ما يتعلق بحياة الشخص المالية أو تعاملاته بيانات شخصية.[2]

(1) Bygrave L. Data Protection Law: "Approaching Its Rationale، Logic and Limits"Coma Press (2002) p. 61.

See also International Privacy Index". Electronic Privacy Information Center (EPIC). 2013.

(2) Krishnamurthy B، Wills CE. On the Leakage of Personally Identifiable Information Via Online Social Networks،، US Press، (2009).P 112

المطلب الثالث

تطور مفهوم البيانات الشخصية

تشكل حقوق الإنسان وحرياته المرجع الرئيس لحماية حرمة حياته الشخصية وهي تبعاً لذلك السند الأساسي لمجموعة الحقوق المتصلة بهذه الحرمة، ويعد موضوع حماية البيانات موضوعا ذا اهتمام دولي لذلك وجب دراسة:

- تطور مفهوم البيانات الشخصية من الناحية القانونية **(الفرع الأول)**.
- ثم لفهم أعمق في ظل التطور التكنولوجي فيجب بحث تطور مثل هذه البيانات من الناحية التقنية**(الفرع الثاني)**.

الفرع الأول

تطور مفهوم البيانات الشخصية من الناحية القانونية

وقد تطوّر هذا المفهوم منذ القدم وبشكل دائم، وقد صدرت بعض النصوص والوثائق مثل الماغنا كارتا عام [1]1215 التي وضعت حدوداً للسلطات السياسية، وتلتها بعد ذلك "المواد الاثنتي عشرة" عام [2]1525 في ألمانيا، ثم إعلان الجمعية الوطنية الفرنسية حول حقوق الإنسان عام1789كوليدة الثورة الفرنسية[3]، وبعدها بعامين صدرت شرعة الحقوق في الولايات المتحدة الأميركية عام 1791[4].

أدخلت هذه النصوص إلى المجتمع والفرد فكرة أن الحقوق الإنسانية تعتبر واجبة الاحترام من الغير ويجب حمايتها قانوناً. فبعد أن كان الإنسان سلعة يباع ويشترى جسديا(العبودية)بدون الالتفات حتى إلى كرامته وفكره، أصبح هو ورأيه وكرامته واحترامه موجباً له على الغير وعلى السلطات الرسمية.

مع هذا الاهتمام المتزايد بحقوق الإنسان أوردت شرعة حقوق الإنسان الصادرة عن الأمم المتحدة في العام 1948 بعد الحرب العالمية الثانية وبسبب

(1) Magna Carta: available at http://en.wikipedia.org/wiki/Magna_Carta p.34

(2) Twelve Articles available at: http://en.wikipedia.org/wiki/Twelve_Articles

(3) Déclaration de Droits de L'Homme et du Citoyen available at http://en.wikipedia.org/wiki/Declaration_of_the_Rights_of_Man_and_of_the_Citizen p.10

(4) United States Bill of Rights: http://en.wikipedia.org/wiki/United_States_Bill_of_Rights p.15

مآسي هذه الأخيرة، مجموعة من الحقوق التي وقعتها الدول المنضمّة إلى الأمم المتحدة وباتت تعتبر قاعدة عامة تقتدي الدول بها، وقد ورد فيها إعلان واضح عن الاعتراف النهائي بالحقوق الفردية للإنسان، لاسيما في المادة 12 من الإعلان التي حددت أن حق الشخص بعدم التعرض العشوائي لخصوصيته، كما لا يجوز التعرض لكرامته.

أمام هذا الواقع، وبعد تطوّر مفهوم الحرية الشخصية في العالم الغربي أولاً حيث تقر المجتمعات بقيمة الحياة الشخصية وحرمتها كإحدى القيم التي لا يجوز التعرض لها والتي يجب صونها، توسع هذا المفهوم أكثر في جميع المجتمعات بنسب متفاوتة، مثل العالم العربي أو الشرقي حيث ما تزال العائلة بمختلف قيمها ركيزة احترام الحقوق والحريات الشخصية.

لذا وإزاء هذا التطوّر، تبين منذ منتصف القرن الماضي، لاسيما في أوروبا، أنّه مع تزايد استعمال أنظمة الحاسوب والحواسيب الكبيرة الفائقة السرعة التي يمكنها حفظ كمية هائلة من البيانات وتداولها بسرعة ليس فقط ضمن إطار دولة واحدة إنما على مستوى دول العالم قاطبة بما في ذلك البيانات الخاصة بالأفراد مثل الاسم، الأصل، العنوان، الآراء والمعتقدات، التفاصيل الطبية تبين للمشرع أن إمكانية الكشف والتقاطع والمعالجة والتحليل لهذه البيانات يعرض الخصوصية الفردية لآثار سلبية، ويمكن التعسف في استعمال هذه الأنظمة وإساءة استخدام البيانات ذات الطابع الشخصي.

أحاطت فرنسا بداية بموضوع البيانات الشخصية ووضعت تشريعاً خاصاً حوله، رقم 17 لسنه 1987 المتعلق بالمعلوماتية وبالملفات وبالحريات متضمناً المبادئ الأساسية في هذا الإطار مبادئ جمع المعلومات، التصريح عن غايات المعالجة، صفات المعلومات، حق الشخص المعني في الاطلاع وطلب التصحيح. كما أنشأ القانون هيئة إدارية مستقلة مهمتها السهر على حسن تطبيق القانون.[1]

(1) Jensen، Carlos Privacy policies as decision - making tools: an evaluation of online privacy notices،Press Releasses، (2004). P90

وقد اعتمد قانون 1978 نموذجاً لاتفاقية المجلس الأوروبي لعام 1981 ولمعظم القوانين الصادرة في الدول الأوروبية لاحقاً.

تتالت بعد ذلك النصوص الأوروبية الوطنية حول الموضوع في السويد والمملكة المتحدة وخلافهما، وتلك الخاصة بالاتحاد الأوروبي كالقرارات والمعاهدات والإرشادات إضافة إلى ذلك، ومع تعاظم حجم التجارة الإلكترونية واتساعها، اتضحت أيضاً القيمة التجارية للبيانات ذات الطابع الشخصي وقد تدخل البرلمان الأوروبي لتفادي إقرار تشريعات متناقضة بين الدول الأوروبية قد لا تعتمد نفس مستوى الحماية القانونية للبيانات ذات الطابع الشخصي، مما قد يعرقل نقل مثل هذه البيانات بين الدول الأوروبية ولاسيما في مجال التجارة الإلكترونية، وكذلك لتأكيد كون أنظمة معالجات البيانات ذات الطابع الشخصي هي في خدمة الإنسان الذي يجب أن تحترم حرياته الأساسية وحقوقه، ولاسيما الحياة الخاصة، مع الأخذ بعين الاعتبار ضرورة المساهمة في التطور الاجتماعي والاقتصادي لذلك عمد البرلمان الأوروبي بعام 1995 إلى إصدار إرشاد للدول الأوروبية يتعلق بحماية الأشخاص الطبيعيين لجهة معالجة البيانات ذات الطابع الشخصي ولجهة حرية نقل هذه البيانات.[1] إن هذا الإرشاد جاء متوافقاً مع السياسة الأوروبية حول حقوق الإنسان كما هي محددة في المعاهدة الخاصة بحماية حقوق الإنسان والحريات الأساسية لعام 1950.

وكذلك مع التوجيهات الصادرة عن منظمة التعاون الاقتصادي والتنمية OECD The Organization for Economic Co - operation and Development عام 1980[2] الخاصة بحماية البيانات التطور ذات الطابع الشخصي ونقلها عبر الحدود وقد عمدت فرنسا

---

(1) http://conventions.coe.int/treaty/fr/Treaties/Html/005.htm

(2) Guidelines on the Protection of Privacy and Transporter flows of Personal data، (1980)، http://www.oecd/document p.34

إلى إدخال الإرشاد الأوروبي المنوه عنه في نظامها القانوني الصادر عن الاتحاد الأوروبي إرشادات[1] وقرارات لاحقة للإرشاد مبنية عليه، وتتعلق بمعالجة أو نقل البيانات ذات الطابع الشخصي عبر الوسائل التقنية والإلكترونية.[2]

من خلال مراجعة هذه النصوص الأحدث نسبياً من الإرشاد من المذكور تبين أنها تستند إلى الإرشاد رقم 95 ناحية المبادئ العامة، إلا أنها تختلف عنه من ناحية بعض النقاط التقنية أو العملية الخاصة بطرق المعالجة أو النقل الخاصة.

وقد تم الاسترشاد بالإرشاد الأوروبي الصادر عام 1995، المتعلق بحماية الأشخاص الطبيعيين لجهة معالجة البيانات ذات الطابع الشخصي ولجهة حرية نقل هذه البيانات وإضافة إلى النصوص اللاحقة التي تكاملت معه، لدى إعداد نص الإرشاد الحالي حول معالجة البيانات ذات الطابع الشخصي، وذلك بالنظر للتراث الأوروبي العريق والتجربة الناجحة في مجال حماية حقوق الإنسان والحريات العامة، وبالنظر أيضاً إلى الانسجام العام بين القوانين الأوروبية ومعظم الأنظمة القانونية العربية، وهي ذات مصدر لاتيني مشترك.[3]

أضف إلى ذلك كون الإرشاد الأوروبي المذكور قد شكل الركيزة

---

(1) Directive 200624//EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 200258//EC p.46

(2) Pfleeger، Charles; Pfleeger، Shari Security in Computing (4th ed.). Boston: Pearson Education(2007).. p. 220

(3) Hugl، Ulrike "Reviewing Person's Value of Privacy of Online Social Networking،" Internet Research، (2011)، p21(4)، in press، http://www.emeraldinsight.com/journals.htm?issn1066 - 2243&volume21&issue4&articleid1926600&showabstract.

القانونية لجميع دول الاتحاد الأوروبي وحتى للدول غير الأوروبية، فقد صدر مبدأ الميناء الآمن" [1] وهو مجموعة مبادئ تُشكل قواعد تصرف على الشركات الأميركية التقيّد بها عند نقل المعلومات إليها من إحدى الدول الأوروبية عندما تكون هذه المعلومات ذات طابع شخصي. إن مبدأ الميناء الآمن قد تم وضعه للتكيّف مع قواعد الإرشاد الأوروبي رقم 95 وهو يتلخص بأن متلقي البيانات ذات الطابع الشخصي إذا كان خارج الاتحاد الأوروبي أي خارج نطاق تطبيق الإرشاد فيجب عليه أن يؤمن مستوى حماية للبيانات ذات الطابع الشخصي ملائماً للإرشاد المذكور [2].

إضافة إلى ما سبق، فبمراجعه القوانين المتعلقة بحماية الخصوصية من خلال العودة إلى الدساتير العربية تبين أن جميع الدساتير كفلت الحرية الشخصية للمواطنين، إلا أن أغلبها بقي صامتاً من ناحية الخصوصية والحياة الشخصية، باستثناء الدستورين المصري والقطري حيث ورد صراحة في المادة 45 من الدستور المصري: إن لحياة المواطنين الخاصة حرمة يحميها القانون. وكذلك ورد في المادة 37 من الدستور القطري)الجديد نسبياً والعائد لعام 2003 (إن لخصوصية الإنسان حرمتها، فلا يجوز تعرض أي شخص لأي تدخل في خصوصياته أو شؤون أسرته أو مسكنه أو مراسلاته

---

(1) Safe Harbor principle: http://en.wikipedia.org/wiki/International_Safe_Harbor_Privacy_Principles: US - EU Safe Harbor is a streamlined process for US companies to comply with the EU Directive 9546//EC on the protection of personal data. Intended for organizations within the EU or US that store customer data، the Safe Harbor Principles are designed to prevent accidental information disclosure or loss. US companies can opt into the program as long as they adhere to the 7 principles outlined in the Directive. The process was developed by the US Department of Commerce in consultation with EU.

(2) http://ec.europa.eu/justice/policies/privacy/modelcontracts/index_en.htm Accessed 232012/5/. P.34

أو أيـة تدخـلات تمـس شرفـه أو سـمعته، إلا وفقـاً لأحـكام القانـون، وبالكيفيـة المنصوص عليهـا فيـه، يتبـين مـن نـص الدسـتور القطـري أنـه جـاء متوافقـاً مـع مبـدأ حمايـة الخصوصيـة وتنظيـم إمكانيـة التعـرض لهـا قانونـاً، مـما يعنـي الإقـرار بالمبـادئ التي جاء الإرشـاد الأوروبي ينـص عليهـا.

تطـور مفهـوم البيانـات الشـخصية بالمعنـى التقنـي جعـل المـشرع يفرد لـه قوانين وتشريعـات خاصـة فكلـما تطـورت التكنولوجيـا زادت الحاجـة إلى قوانـين تضـع إطـارا للممارسـات المختلفـة.[1]

---

(1) Popa، C.، et. all.، "Managing Personal Information: Insights on Corporate Risk and Opportunity for Privacy - Savvy Leaders"، Carswell (2012)، Ch.6

الفرع الثاني

تطور مفهوم البيانات الشخصية من الناحية التقنية

بعدما انغمست فكره حماية البيانات الشخصية داخل قوانين الخصوصية لفترة طويلة أصبحت الآن موضوعا منفصلا يفرد لها القوانين الخاصة به ولكن لم يطبق ذلك بعد في جميع دول العالم.

فبعدما كانت البيانات الشخصية تقتصر على الاسم والعنوان والتليفون، ونظرا للتطور التكنولوجي في مناحي الحياة أصبحت الصورة الشخصية والفيديوهات التي يتم التقاطها للشخص تعتبر بيانات شخصية.[1]

وقد ظهر مؤخرا مصطلح علم المقاييس الحيوية وهو يعرف بـ:

علم الأدلة الجنائية في الأجسام البشرية لأنه يضم وسائل التعرف علي الهوية للأشخاص تلقائيا علي أساس الصفات الفسيولوجية والتشريحية الخاصة لكل شخص. وأكثر هذه الأدلة شيوعا بصمات الأصابع ويمكن لأجهزة الكمبيوتر مضاهاتها في ثوان.

كما يمكن أيضا التعرف علي هويتك من خلال ملامح الوجه أو الصوت أو هندسة اليد أو حدقة العين. وكل أجهزة المقاييس الحيوية (Biometrics) تستخدم كل المبادئ العامة.[2]

وهذه المقاييس تعالج من خلال البرمجة والتشفير للسمات الفريدة لكل

---

(1) Privacy Commissioner's Report of Findings، "Law School Admission Council Investigation " May 29، (2008) p.23

(2) Jain، A.، Hong، L.، & Pankanti، S. "Biometric Identification". Communications of the ACM، (2000). p. 91 - 98.

شـخص، وتخـزن في قاعـدة البيانـات لمضاهاتهـا بملامـح وسـمات المشـتبه فيهـم. لهـذا نجـد أن نظـم المعلومـات في وسـائل المقاييـس الحيويـة تعتـبر وسـيلة سريعـة ودقيقـة.

ويمكـن اسـتخدام أكـثر مـن وسـيلة بهـا للتعـرف عـلي هويـة الشـخص 100%. فعندمـا توجـد جريمـة فالعلـم وراءهـا بالمرصـاد للكشـف عـن مصادرهـا وفاعليهـا.[1]

ومـن ثـم فـإن البيانـات الشـخصية البيومتريـة قـد تعتمـد بصفـه أساسـية عـلى مواصفـات الشـخص الفسـيولوجية مثـل بصمـة الأصابـع وبصمـة العـين والصـوت.

وبالرغـم مـن أن تلـك البيانـات لا تضـع توصيفـا محـددا للشـخص فإنهـا عـاده تسـتخدم للتأكـد مـن هويـة الشـخص عـن طريـق سـهوله التعريـف الشـخصي عـن طريق البيانـات الشـخصية البيومتريـة حيـث إنهـا لا تتشـابه بـين شـخص وآخـر وتدخـل البصمة الوراثيـة أيضـا ضمـن قائمـه البيانـات الشـخصية البيومتريـة.[2]

وتعتـبر البيانـات الناتجـة عـن تتبـع أحـد الأشـخاص بواسـطة (GPS) [3] والموجود في أحـد السـيارات - بيانـات شـخصية طالمـا تـم ربطهـا بشـخص معين سـواء كان السـائق أو الراكب [4].

(1) Jain، Anil K.; Ross، Arun (2008). "Introduction to Biometrics". In Jain، AK; Flynn; Ross، A. Handbook of Biometrics. Springer. pp. 1–22 See also Jain، A.K.; Bolle، R.; Pankanti، S.، eds. Biometrics: Personal Identification in Networked Society. Kluwer Academic Publications(1999).

(2) Weaver، A.C. (2006). "Biometric Authentication". Computer، 39 (2)، p. 96 - 97. DOI 10.1109/MC.2006.47

(3) GPS: Global Positioning System

(4) https: // www. priv. gc. ca/ leg _ c/ interpretations _ 02 _ e.asp Accessed 23/ 12/ 2013 p. 10

وتعتبر البيانات المجمعة من خلال أنظمة تحديد الهوية والمعلومات بواسطة موجات الراديو (RFID) [1] والمخصصة لتتبع البضائع والمنتجات وبتحديد المشتري لمثل هذه البضائع يعد بيانا شخصيا للمشتري.[2]

أيضاً عنوان بروتوكول الإنترنت (IP address) وهو رقم التعريف بالجهاز المتصل بشبكه ما ويستطيع مقدم خدمه الإنترنت (ISP) تحديد عنوان بروتوكول الإنترنت عن طريق اسم التعريف الخاص بكل مستخدم ويعتبر من البيانات الشخصية وذلك إذا ارتبطت بشخص معرف أو محدد أو قابل للتعريف كذلك يمكن أن يكون عنوان بروتوكول الإنترنت بيانا شخصيا لأكثر من شخص في الوقت ذاته إذا كان الجهاز صاحب العنوان يستخدم بواسطة أكثر من شخص. [3]

---

(1) رقائق ال RFID تكون على شكل بطاقات يمكن لصقها أو تثبيتها على الأشياء، وهذه الرقائق الصغيرة جداً تحتوي على هوائي لاستقبال الموجات والذي يكون على شكل سلك رفيع ملفوف داخل البطاقة. يقوم هذا الهوائي باستقبال الموجات المغناطيسية الصادرة من جهاز القراءة ويشغل الدائرة الإلكترونية الموجودة داخل البطاقة والتي بدورها تبدأ عملية البث اللاسلكي للقارئ وتصل المعلومات عند نقلها إلى جهاز الحاسوب أو الشبكة في النهاية. كما ذكرنا سابقاً فإن بطاقات RFID تحتوي على ذاكرة بخلاف الرقم المرمز Barcode الذي يحتوي فقط على رقم يرسل للقارئ، هذه الذاكرة الصغيرة (عادة من نوع EEPROM) تتسع لمعلومات مفصلة وقد تصل سعتها إلى 256 بايت. لابد أن نلاحظ أن هذه الرقاقة لا تحتوي على مصدر طاقة خاص بها (بطارية مثلاً) وذلك يسهل وضعها على البضائع، ولكن هذه التقنية تعمل على مبدأ دوائر الرنين (resonance circuit) والتي تقوم باستخدام طاقة الموجات الكهرومغناطيسية الصادرة عن جهاز القراءة، تتكون الدائرة بشكل بسيط من ملف ومكثّف (Coil and Capacitor) وتصل الدائرة إلى مرحلة الرنين عند توافق تردد موجات القارئ وتردد الدائرة فتستخدم الطاقة الناتجة لإرسال المعلومات للقارئ. يقوم القارئ بدوره بتحويل الإشارات اللاسلكية الواصلة من البطاقة إلى بيانات رقمية قابلة للتعامل بالحاسوب حيث تتم معالجتها بالبرامج

(2) Radio Frequency Identification (RFID) in the Workplace: Recommendations for Good Practices، Office of the Privacy Commissioner of Canada، A consultation Paper (March 2008) p.112.

(3) What an IP Address Can Reveal About You، a report prepared by the Technology Analysis Branch of the Office of the Privacy Commissioner of Canada، (May 2013) p.134.

مما لا شك فيه أننا نعيش في عصر من التكنولوجيا التي أتاحت استخدام المواقع الإلكترونية الاجتماعية أو ما يعرف ب (Social Media) مثل الفيسبوك[1] (facebook) والتويتر (Twitter) والبلاك بيري (Black Berry) وما تتميز به من سرعة تبادل الأخبار والمعلومات بين المشتركين، مما سهل من فرص انتهاك الخصوصية الشخصية من خلال نشر الشائعات وتداولها بشكل مطرد سريع يصعب من الحد منه أو القضاء عليه وغيرها من صور انتهاك الخصوصية الرقمية.[2]

و تعرف الخصوصية الرقمية بأنها عدم التعدي على البيانات الشخصية عبر الإنترنت أو أي وسيط مماثل ويكون انتهاكا للخصوصية الرقمية كل تعدي على البيانات الشخصية الموجودة على شبكة الإنترنت بالمعالجة أو الاستيلاء والاستخدام.[3]

هناك نوع من المعلومات يطلق عليها خاصة كونها تتعلق بالشخص ذاته وتنتمي إلى كيانه كإنسان مثل الاسم والعنوان ورقم الهاتف وغيرها من المعلومات، فهي معلومات تأخذ شكل بيانات تلزم الالتصاق بكل شخص طبيعي معرف أو قابل للتعريف [4].

وهذه النوعية من المعلومات أصبحت في وقتنا الحاضر على درجة كبيرة

---

(1) Grimmelmann، James "Saving Facebook". Iowa Law Review(2009).. pp. 1137-1206

(2) Larose، R.، & Rifon، N. J. (2007). Promoting i - Safety: Effects of Privacy Warnings and Privacy Seals on Risk Assessment and Online Privacy Behavior. Journal Of Consumer Affairs، 41(1)، 127-149.

(3) Miller، Vincent Understanding digital culture. "Convergence and the contemporary media experience". London: Sage Publications (2011) P 102

(4) الدكتور. عمر أبو بكر بن يونس، الجرائم الناشئة عن استخدام الإنترنت - دار النهضة العربية، القاهرة 2004 ص 614

مـن الأهميـة في ظـل فلسـفة المعلوماتيـة المعـاصرة، سـيما وأن فكـرة العـالم الرقمـي، لا يمكـن لهـا السـير في التطـور ومواكبـة اهتمامـات الإنسـان سـوى باسـتخدام المعلومـات. مـن هنـا ظهـر مـا يعـرف بالخصوصيـة المعلوماتيـة.[1]

و خـلال الربـع الأخـير مـن القـرن التاسـع عـشر حيـث أشـار إلى مبـدأ الخصوصية المعلوماتيـة كلا مـن المؤلفـين الأمريكيـين الخبيريـن في هـذا الحقـل، وهـما الأول في كتـاب الخصوصيـة والحريـة Privacy and Freedomلمؤلفـه ويسـتن - Alan Westin عـام1967[2]، والثـاني كتـاب الاعتـداء عـلى الخصوصيـة The Assault on Privacy لمؤلفـه ميلـر[3] Miller، وكلاهـما قدمـا مفهومـا وتعريفـا لخصوصيـة المعلومـات.

فويسـتن ذهـب في تعريفـه للخصوصية المعلوماتيـة إلى أنها: "حق الأفـراد في تحديد متـى وكيـف والى أي مـدى تصـل المعلومات عنهـم للآخرين.

The claim of individuals 'to determine for themselves when، how)

(and to what extent information about them is communicated to others

في حـين عـَرف ميلـر الحـق في خصوصيـة المعلومـات: عـلى أنهـا قـدرة الأفـراد عـلى التحكـم بـدورة المعلومـات التـي تتعلـق بهـم.

---

(1) Mediati، N. (2010). The Most Dangerous Places on the Web. PC World، 28(11)، 72–80

(2) Westin، A F، Privacy and Freedom، New York، Atheneum. (1967) p.12

مشار إليه في د. يونس عرب دور حماية الخصوصية في تشجيع الاندماج بالمجتمع الرقمي - ورقة عمل مقدمة إلي ندوة أخلاق المعلومات - نادي المعلومات العربي – 16 - 17 أكتوبر 2002 – عمان – الأردن

(3) Miller، A.، “The Assault on Privacy”، Ann Arbor، University of Michigan Press (1971) p.12.

(The individual's ability to control the circulation of information relating to. him')

ويمكن القول: إن الخصوصية من حيث مفهومها جرى التعامل معها كحق لمنع إساءة استخدام الحكومة للبيانات التي يصار لمعالجتها آليا أو الكترونيا أو تقييد استخدامها وفق القانون فقط [1].

أما على صعيد التشريع فقد شهدت أوروبا تطوير هذه الفكرة ضمن حزمة شاملة من مبادئ السلوك والممارسات المقبولة، أهمها تأكيد الاستخدام العادل والمنصف للبيانات الشخصية، والتدخل بالحدود الدنيا، وتقييد وتضييق أغراض استخدام البيانات وحصر الاستخدام في غرض الجمع.[2]

خلاصة الأمر يمكننا القول: إن خصوصية المعلومات هي حماية البيانات، فهناك ترادف بوجه عام قائم ما بين اصطلاح خصوصية المعلومات وحماية البيانات، وليس بين الخصوصية وبين حماية البيانات.

أما شيوع استخدام اصطلاح الخصوصية مستقلا ومنفردا دون إلحاقه بالبيانات في البيئة الإلكترونية للدلالة على حماية البيانات واستخدامه كذلك في الدراسات الأكاديمية وفي الدراسات التقنية وأبحاث وتقرير قطاعات الأعمال، فهو أمر يرجع إلى أن تعبير الخصوصية شاع بوقعه هذا في ظل تزايد مخاطر التقنية إلى مدى ارتبط بها في الاستخدام وكأنه ينحصر في نطاقها وبيئتها، وهو طبعا ليس كذلك، لكن ربما لأن أشد ما يمكن أن يمثل تغولا على هذا الحق وانتهاكا له، هو الوسائل التقنية ومخاطر المعالجة الآلية للبيانات.

كما أن استخدام اصطلاح الخصوصية في بيئة مواقع الإنترنت ومسائل

(1) الدكتور يونس عرب: الخصوصية وحماية البيانات، بحث منشور على شبكة الإنترنت من خلال موقع www.arablaw.net ص 12

(2) Guadamuz A، 'Habeas Data: The Latin - American Response to Data Protection'، The Journal of Information، Law and Technology (JILT 2000) (2) p.132. <http://elj.warwick.ac.uk/jilt/00 - 2/ guadamuz.html

عقود التقنية أو خدمات التقنية عموما يشير إلى حماية الخصوصية المعلوماتية أو حماية البيانات.[1]

و قد تطور مفهوم البيانات الشخصية المتداولة عبر الإنترنت فقد عرفت على أنها البيانات أو (البيانات التوصيفية) التي أنشأها الشخص أو قام غيره بإنشائها لشخصه وتشمل [2]

1. البيانات الطواعية:

وهي البيانات التي يدرجها الشخص طواعية ويتشاركها مع غيره عبر مواقع التواصل الاجتماعي بداية من الاسم والعنوان والتليفون والبريد الإلكتروني والصور وكذلك الأخبار اليومية والحياتية التي يتشاركها مع غيره من المستخدمين، ويعتبر الرقم السري لبطاقة الائتمان من البيانات الشخصية التي يتنازل عنها الشخص ما إذا قام بشراء المنتجات عبر الإنترنت.

2. البيانات المرصودة:

وهنا يتم الحصول على هذا النوع من البيانات عن طريق التتبع والرصد مثل تحديد الأماكن التي يتم من خلالها إرسال رسائل البريد الإلكتروني.

3. البيانات الاستدلالية:

هي البيانات الشخصية الناتجة من تحليل البيانات المرصودة والبيانات الطواعية ونتائج هذه التحليلات تعتبر بيانات شخصية لارتباطها بالأشخاص الذين تم تتبعهم أو رصد وتحليل بياناتهم.

---

(1) الدكتور يونس عرب: الخصوصية وحماية البيانات، بحث منشور على شبكة الإنترنت من خلال موقع www.arablaw.net ص 12

(2) Mediati، N. The Most Dangerous Places on the Web. PC World، (2010). 72-80.

وفي هـذا الصـدد فـإن القوانـين والمواثيـق الدوليـة متفقـة عـلى تجريـم جميـع أشـكال انتهـاك الخصوصيـة المعلوماتيـة للفـرد ومـا قـد يترتـب عـلى ذلـك مـن عقاب مع اختـلاف جـذري في تحديـد مـا يمكـن أن يطلـق عليـه انتهـاكا في ذلـك الخصـوص، ولكـن الإشـكالية هنـا تـبرز في مـدى إمكانيـة إنـزال تلكـم العقوبـات الجزائية على واقـع المواقع الاجتماعيـة الإلكترونيـة (Social Media) وذلـك لكـثرة المسـتخدمين واختـلاف أماكنهـم وتعـدد ثقافاتهـم وصعوبـة (في بعـض الأحيـان) تحديـد ومعرفة الهويـة الحقيقية لمنشـئ الصفحـة أو المدونـة الإلكترونيـة والقائمـين عليهـا... وأهدافهـم وانتماءاتهـم العرقيـة والعقائديـة والثقافيـة.[1]

---

(1) Krishnamurthy B، Wills CE. On the Leakage of Personally Identifiable Information Via Online Social Networks، HG press، (2009).P 76

See also Soltani، Ashkan. "Flash Cookies and Privacy". University of California، Berkeley. Retrieved 3 February 2012.

الفصل الثاني

الحماية القانونية للبيانات الشخصية

المبحث الأول: التوجهات التشريعية لحماية الخصوصية المعلوماتية.

المبحث الثاني: تاريخ القوانين التي تحكم خصوصية البيانات في القوانين المقارنة.

المبحث الثالث: الجهود الدولية والإقليمية لحماية الخصوصية المعلوماتية.

المبحث الأول

التوجهات التشريعية لحماية الخصوصية المعلوماتية

للخصوصية وفق تطورها التاريخي ثلاث محطات رئيسة، بداية الاعتراف بالخصوصية كحق لحماية الأفراد من مظاهر الاعتداء المادي على حياتهم وممتلكاتهم، وهي ما تعرف بالخصوصية المادية ثم انطواء الخصوصية على حماية القيم والعناصر المعنوية للشخص، وهي ما عرف بالخصوصية المعنوية، وبعد ذلك أصبحت الخصوصية كحق عام يمتد نطاقه لحماية الشخص من كافة أوجه الاعتداءات والتدخل في حياته أيا كان مظهرها أو طبيعتها، وفي نطاق المعنى الأخير ولد مفهوم جديد للخصوصية ارتبط بأثر التقنية على الحياة الخاصة، تمثل بخصوصية المعلومات أو حق الأفراد في السيطرة على المعلومات والبيانات الخاصة في مواجهة تحديات العصر الرقمي.

ومن هنا يمكن القول بأن كافة دول العالم على وجه التقريب أقرت بشكل أو بآخر الحق في الخصوصية في واحد أو أكثر من مظاهره، وهذا لا يعني توفر حماية كافية، أو شمولية في الحماية لدى كافة الدول، وفي الوقت الذي قد نجد فيه حماية الخصوصية بمفهومها المادي أكثر شيوعا واتساعا، تضيق حماية خصوصية المعلومات، وفي الوقت ذاته نجدها الشغل الشاغل في الوقت الحاضر للمؤسسات التشريعية ومؤسسات القرار في العديد من دول العالم.[1]

- ومن هنا تحتم عرض تاريخ تشريعات الخصوصية وإطارها العام **(المطلب الأول)**.

---

(1) Krisana Kitiyadisai، "Privacy Rights and Protection: Foreign Values in Modern Thai Context"، springerlink، March (2005) p.121.

- وكذلك الأنماط والنماذج التشريعية في حقل حماية البيانات (**المطلب الثاني**).
- وأخيرا الإطار العام للقوانين التي تحمي الخصوصية في الدول العربية (**المطلب الثالث**).

المطلب الأول

تاريخ تشريعات الخصوصية وإطارها العام

إن النصوص الدستورية وفي حدودها الدنيا، نصت على الحق في حرمة المسكن والحق في سرية المراسلات (الخصوصية المادية) ويلاحظ أن الدساتير الحديثة - كما في دساتير أوروبا في التسعينات - نصت صراحة على الحق في وصول وسيطرة الشخص على بياناته الشخصية (خصوصية المعلومات)(1) وحتى في الدول التي لا تتضمن دساتيرها نصوصا دستورية صريحة بشأن الحق في الخصوصية، كما في الولايات المتحدة وايرلندا والهند وغيرها.(2)

- ولبحث فكرة نشأة الخصوصية يجب عرض تاريخ القوانين التي عالجت تلك الفكرة (**الفرع الأول**).
- ثم ارتباط تطور خصوصية البيانات بتطور تقنية المعلومات (**الفرع الثاني**).
- وبعد ذلك الأوصاف العامة لتشريعات خصوصية البيانات (**الفرع الثالث**).

---

(1) Patrick Wintour، "EU scraps timetable for ratifying constitution"، The Guardian press (London)، 2005 P 76

(2) Regulation of the Cloud in India، Ryan، Falvey & Merchant، Journal of Internet Law، Vol 15، No. 4 (October 2011). See also Invasion of privacy: penalties and remedies: review of the law of privacy: stage 3" (2009) (Issues paper 14)، New Zealand Law Commission،

الفرع الأول

تاريخ قوانين خصوصية البيانات

وبذلك فإن الحق في الخصوصية متضمن ومقر ضمن النصوص التي تتعلق بحقوق دستورية أخرى، وفي دول أخرى، يمثل الانضمام والمصادقة على الاتفاقيات الدولية التي اعترفت بهذا الحق، مصدرا للحق الدستوري، عندما تتقدم نصوص هذه الاتفاقيات على القوانين العادية.

وقد شهدت الستينات انطلاق الاهتمام بحماية الخصوصية من مخاطر التكنولوجيات الحديثة، لينطلق معه مفهوم حماية البيانات الخاصة من مخاطر التقنية، ومنذ مطلع السبعينات بدأت دول العالم تتبنى قوانين حماية الخصوصية إما عن طريق القوانين الشمولية التي تعترف بالحق وتقر المبادئ الأساسية وتقدم الإطار القانوني الموضوعي والإجرائي لحماية خصوصية المعلومات أو حماية البيانات التي تتصل بالأفراد وحياتهم الخاصة (البيانات الشخصية)، أو عن طريق حزمة قوانين قطاعية تتعلق بالبيانات في قطاعات معينة، كالبيانات الصحية أو المالية أو بيانات الأحوال المدنية أو غيرها، إلى جانب مدونات سلوك تحكم قطاعات معينة كقطاعات الصناعة أو الخدمات التقنية فيما يعرف بوسيلة التنظيم القانوني الذاتي للقطاعات أو السوق.[1]

وغالبية هذه القوانين إن لم تكن كلها اعتمدت في محتواها وما تضمنته على قرارات مجلس أوروبا عامي 73 و74 واتفاقية (مجلس أوروبا) الخاصة بحماية البيانات من مخاطر المعالجة الآلية لعام 1980،[2] وعلى دليل منظمة

(1) Bergstein، Brian "Research explores data mining، privacy". USA Today Press (2006 P 67)

(2) Carroll، Joe (31 December 1986). "Single Act ratified by 11 states". The Irish Times. p. 13

التعاون الاقتصادي والتنمية لعام 1980 ودليل الأمم المتحدة اللاحق عام 1990، وفي تطورها وشموليتها خلال السنوات الأخيرة اعتمدت بشكل واضح على تعليمات توجيه للاتحاد الأوروبي لحماية البيانات عام 1995.

وبالعودة للتوجيه الصادرة عن الاتحاد الأوروبي عام بشأن حماية البيانات 1995، وفي نقلة نوعية مثلت تكريسا لمفهوم خصوصية المعلومات وإقامة التوازن بين هذا الحق والحق في تدفق المعلومات عبر الحدود ومواجهة تحديات توظيف التكنولوجيا في الأنشطة الإدارية والإنتاجية والخدمية في الدولة، اصدر الاتحاد الأوروبي في عام 1995 دليلا شاملا - ملزما لدول الاتحاد الأوروبي، ولهذا نطلق عليه الأمر التشريعي ويسميه البعض قانونا أو تعليمات - يتعلق بحماية خصوصية المعلومات وتنظيم نقل المعلومات خارج الحدود، وقد أقر من قبل البرلمان الأوروبي ومجلس أوروبا معا.

وتبعه عام 1997 دليل آخر لتنظيم معالجة البيانات الشخصية في قطاع الاتصالات، وهذا الجهد الجديد - مضافا إليه استمرار الجهود من قبل أطر الأمم المتحدة ومؤسسات أوروبا الموحدة ومنظمة التعاون الاقتصادي والتنمية عبر إصدار أدلة متعددة تعالج مختلف طوائف البيانات وحمايتها في البيئة الرقمية - جاء معتمدا على النشاط السابق الذي أنتج المدونات المشار إليها أعلاه، وتميز الأمر التشريعي للاتحاد الأوروبي لعام 1995 بإلزام الدول الأوروبية بإدماجه ضمن تشريعاتها في فترة أقصاها نهاية أكتوبر 1998،[1] وهو ما أدى إلى موجة تشريعية جديدة وموجة تعديل التدابير التشريعية القائمة في مختلف دول أوروبا، وتحديدا الدول الخمسة عشرة الأعضاء في الاتحاد، وأثر ذلك على عشرات دول العالم من خارج أوروبا التي وجدت في هذه التجربة الناضجة لحماية البيانات الشخصية هاديا لها ونموذجا متقدما

(1) Kamaal Zaidi، Harmonizing U.S. - EU Online Privacy Law: Toward a U.S. Comprehensive Regime For the Protection of Personal Data، p. 169 (2003).

أمكنهـا الاعتـماد عليـه لإقـرار تشريعـات حمايـة البيانـات الشـخصية أو تشريعـات الخصوصيـة الشـمولية في دولهـا.[1]

وإلى جانـب هـذا الجهـد، ومنـذ السـبعينات أيضـا، تبلـورت جهـود مميـزة في ميـدان حـق الوصـول للمعلومـات وتحديـدا حـق العامـة في الوصـول إلى الوثائـق التـي تحوزهـا أو تملكهـا السـلطات العامـة، وظهـر في غالبيـة المراحـل أن الحكومـات والأطـر الإقليميـة غير متشـجعة لإقـرار هـذا الحـق بالقـدر ذاتـه الـذي جـرى فيـه العمـل عـلى تنظيـم الحـق في الخصوصيـة، لكـن دخـول أوروبـا مرحلـة جديـدة في ظـل حزمـة الاتفاقيـات التـي أنشـأت هيئـات أوروبـا الموحـدة وأنشـأت السـوق الأوروبية المشـتركة، والنـص صراحـة عـلى حـق مواطنـي الاتحـاد الأوروبي في الوصـول إلى وثائـق مؤسسـات أوروبـا ممثلـة بالبرلمـان والمجلـس واللجنـة الأوروبيـة، أوجـب التحرك لإقرار نظـام قانوني للوصـول للمعلومـات، وترافـق هـذا الجهـد وسـبقه أيضـا، قـرارات صـادرة عـن المحكمـة الأوروبيـة بهـذا الاتجـاه.[2]

إضافـة إلى قـرارات صـادرة خارج أوروبا كما في اليابان وشرق آسـيا وأمريكا بشـأن الحـق في الوصـول للسـجلات والوثائق الحكوميـة مضافا إليه تجربة سـابقة لدى عدد من الـدول كأمريـكا وغيرهـا مـن أجـل إتاحـة وصـول العمـوم للبيانـات والوثائق ضمـن قيود وضوابـط مقـررة قانونـا وأدت هـذه التطـورات إلى اتجـاه العديـد مـن الـدول إلى إقـرار تشريعـات شـاملة ومسـتقلة للسـماح بالوصـول للمعلومـات إلى جانـب عـشرات النصوص في العديـد مـن دول العـالم التـي أخـذت بتطبيـق أو أكـثر مـن التطبيقـات المتصلـة بهـذا الحـق، والجامـع المشـترك بينهـا في علاقتهـا بالخصوصيـة، أن حـق الوصـول للمعلومـات

---

(1) Formholz،JuliaM،"European Union Data Privacy Directive"، 15Berk Tech، (2000) p.36 see also William J. Clinton & Albert Gore، Jr.، A Framework for Global Electronic Commerce، FRT Publishing، 1997.

(2) Shmatikov، V. "Myths and fallacies of "personally identifiable information،Communications of the ACM (2010). P 24

يستثنى منه عادة طوائف معينة من المعلومات، في مقدمتها البيانات الشخصية، وذلك حماية لخصوصية الأفراد، إضافة إلى استثناء الوصول لمعلومات معينة لاعتبارات المصلحة العامة والأمن وللعلاقة بالغير أو لحماية الأسرار التجارية أو غير ذلك.(1)

ولأن التوازن بين الحق في حماية البيانات الخاصة وفق مبادئ الخصوصية المتصلة بأنشطة جمع ومعالجة وكشف هذه البيانات، وبين الحق في الوصول للمعلومات، يتطلب إقرار معيار توازن مقبول لأن الخصوصية في حقيقتها قيد على حق الوصول للمعلومات، وهذا أدى إلى إعادة دراسة التجربتين وتقييمهما معا من قبل هيئات حماية البيانات الشخصية وجهات المعلوماتية في النظم المقارنة، وأصبح خير موضع لبحثهما الجهات ذات العلاقة بمسائل المعلوماتية أو تقنية المعلومات أو الجهات المعنية بسياسات المعلومات والكمبيوتر والاتصالات، واتجهت غالبية الدول إلى إقرار التشريعات في الحقلين كل على استقلال.(2)

وساهم في ذلك أن التوجيه الأوروبي لعام 1995 نظم حماية البيانات الشخصية وفي الوقت نفسه الحق في نقل البيانات خارج الحدود وهو جزء من مسائل الحق في الوصول للمعلومات، ووجدت بعض الدول، حتى مع وجود التشريعين كل على استقلال، إن الجهة المعنية بأحكامهما معا يتعين أن تكون جهة واحدة، لهذا مثلا نجد توجها لإناطة صلاحيات مراقبة ومتابعة

(1) يونس عرب، دور حماية الخصوصية في تشجيع الاندماج في المجتمع الرقمي ورقه عمل مقدمة إلى: ندوة أخلاق المعلومات - نادي المعلومات العربي – 16 - 17 أكتوبر 2002 – عمان – الأردن ص134

(2) Brain W.A، Legal Analysis of a Single Market for the Information Society، citation Eropian 2011 P 4 See also Guidelines on the Protection of Privacy and Transborder Flows of Personal Data، available at http://www.oecd.org/document/18/0،2340،en_2649_34255_1815186_1_1_1_1،00. htm retriveied 2 - 12 - 1013

مسائل الحق في الوصول للمعلومات لجهات (مفوضي) حماية البيانات المنشأة بموجب قوانين حماية البيانات،[1] كما هو الشأن في بريطانيا، فقد قامت بريطانيا عام 1998 بتسمية جهة الرقابة على حماية البيانات الشخصية بمفوض حماية البيانات في أعقاب قانون حماية البيانات البريطاني لعام 1998، (وكذلك صدور قانون حقوق الإنسان البريطاني عام 1998) بدل مفوض تسجيل البيانات الذي أنشئ بموجب قانون حماية البيانات عام 1984.

وبصدور قانون حرية المعلومات البريطاني لعام 2000 أيضا، جرى تعديل قانون حماية البيانات لعام 1998 في مسائل عديدة منها: إعادة تسمية مفوض حماية البيانات ومحكمة البيانات المنشأتين بموجب قانون 1998 ليصبحا مفوض المعلومات، ومحكمة المعلومات، مسندة لهما اختصاصات تتعلق بالحقين معا: حماية البيانات الشخصية (الخصوصية) وحرية المعلومات (الحق في الوصول للمعلومات والسجلات) وهو توجه أريد منه إيجاد جهة واحدة تباشر مهام متعددة بالنسبة المعلومات، سواء حق الوصول إليها أم حق حظر المساس بالبيانات الشخصية منها لضمان عدم اختلال معيار التوازن لدى مباشرة الحقين.[2]

(1) Albert Gore، Jr.، A Framework for Global Electronic Commerce، July 1، 1997

(2) MacDonald، Jones،The Law of Freedom of Information BBC press، 2003 P40

الفرع الثاني

خصوصية البيانات وقوانين تقنية المعلومات

الحقيقة إن تقنية المعلومات خضعت منذ السبعينات لموجات متعاقبة من التشريع القانوني في مختلف فروع القانون فنتج عن ذلك ولادة قانون الكمبيوتر أو قانون تقنية المعلومات أو لنقل ملامحه الأولى بدأ مع شيوع استعمال الكمبيوتر وانخفاض كلفه، ولأنه أداة جمع ومعالجة للمعلومات فقد كانت أول تحدياته القانونية إساءة الاستخدام على نحو يضر بمصالح الأفراد والمؤسسات، ومعه نشأ الارتباط بين القانون والكمبيوتر الذي انطلق من التساؤل فيما إذا كانت أنشطة إساءة استخدام الكمبيوتر تقيم مسؤولية قانونية أو أنها مجرد فعل غير مرغوب به أخلاقيا؟ وما إذا كان يتعين تنظيم استخدام الكمبيوتر أو لا ؟؟

وهذا التساؤل أثير في حقلين:

الأول: المسؤولية عن المساس بالأفراد والمؤسسات عند إساءة التعامل مع بياناتهم الشخصية المخزنة في نظم الكمبيوتر على نحو يمس أسرارهم وحقهم في الخصوصية.[1]

والثاني: المسؤولية عن الأفعال التي تمس أو تعتدي على أموال الأفراد ومصالحهم وعلى حقهم في المعلومات ذات القيمة الاقتصادية، ولو دققنا في هذين الحقلين لوجدنا أنفسنا أمام (الخصوصية) و(جرائم الكمبيوتر).

---

(1) Richardson، R.،CSI Computer Crime & Security Survey. Computer Security Institute. (2010). See also J. C. Willemssen، "FAA Computer Security". GAO/T - AIMD - 00 - 330. Presented at Committee on Science، House of Representatives، 2000. See also de Silva، Richard "Government vs. Commerce: The Cyber Security Industry and You (Part One)". Defence IQ(11 Oct 2011). 2014.

إذن ثمة حقيقة أولى هي أن ولادة قانون الكمبيوتر ارتبط بالبحث في المسؤولية عن أنشطة تتصل بالمعلومات ونظمها وتحديدا في الحقل الجزائي.

والجدل الذي دار في ذلك الوقت (الستينات تحديدا وامتد إلى مطلع السبعينات) أشبه بالجدل الدائر في السنوات الأخيرة بشأن الإنترنت هل يتعين إخضاع التقنية الجديدة - توظيفها واستخدامها - للتنظيم القانوني أو تترك للتنظيم الذاتي، أو كما يعبر عنه الفكر الرأسمالي (تنظيم السوق نفسه) فلا نكون أمام قواعد قانونية تقر من الأطر الحاكمة بل أمام قواعد سلوكية وشروط عقدية تتدخل قطاعات الأعمال لوضعها.

في هذا الإطار فإن أول حالة موثقة لإساءة استخدام الكمبيوتر ترجع إلى عام 1958 قام أحد المهندسين بالاستيلاء والاختلاس والتلاعب في بيانات أحد البنوك وفقا لما نشره معهد ستانفورد في الولايات المتحدة الأمريكية[1]، ليبقى الحديث من ذلك الوقت وحتى مطلع السبعينات في إطار البعد الأخلاقي وقواعد السلوك المتعين أن تحكم استخدام الكمبيوتر، ولتنطلق التشريعات الوطنية في حقل جرائم الكمبيوتر مع نهاية السبعينات (تحديدا في الولايات المتحدة ابتداء من 1978)[2].

أما الجهد الدولي فقد تحقق ابتداء في حقل الخصوصية أو حماية الحياة الخاصة من مخاطر التكنولوجيا، ففي عام 1968 شهد مؤتمر الأمم المتحدة لحقوق الإنسان (مؤتمر طهران)، طرح موضوع مخاطر التكنولوجيا على الحق

---

(1) Kang Shuhua، comprehensively building a moderately prosperous society in Crime،Chaniees 1991: pp.322 - 323 See also Den، Marc L.، and Stephanie E. Lucas،Accidents On the Information Superhighway: On - Line،Liability and Regulation، (1996). see also Denning، Dorothy E. (1990). Concerning Hackers Who Break into Computer Systems

(2) Jaishankar، K. (Ed.) Cyber Criminology: Exploring Internet Crimes and Criminal behavior. Boca Raton، FL، USA: CRC Press، Taylor and Francis Group(2011).

في الخصوصية[1]، والذي استتبعه إصدار الأمم المتحدة قرارات في هذا الحقل لتشهد بداية السبعينات (تحديدا عام 1973 في السويد) انطلاق تشريعات قوانين حماية الخصوصية مع الإشارة إلى أنها نوقشت في نظم قانونية أجنبية كثيرة ضمن مفهوم حماية البيانات Data Protection.

فإن الخصوصية وحماية البيانات تمثل أول حقل من حقول قانون الكمبيوتر من حيث الاهتمام التنظيمي الدولي مع أنها ترافقت مع الحديث حول جرائم الكمبيوتر وكما يظهر من تواريخ انطلاق التشريعات الوطنية فإنهما سارا معا من حيث التدابير التشريعية الوطنية مع أسبقية لتشريعات الخصوصية طبعا مع موجة تشريعات الحماية القانونية للبرمجيات.

ولأن السبعينات شهدت بحق الإدراك العميق لأهمية برامج الكمبيوتر وباتت تشير إلى أنها ستكون القيمة الأكثر أهمية من بين عناصر تقنية المعلومات وستفوق عتاد الكمبيوتر المادي في أهميتها، فإن مطلع السبعينات شهد جدلا واسعا حول موقع حماية برامج الكمبيوتر، أهي قوانين براءات الاختراع بوصف البرنامج من المصنفات القابلة للاستثمار في حقل صناعات الكمبيوتر أم أنها تشريعات حق المؤلف باعتبار البرنامج في الأساس ترتيب منطقي لأوامر كتابية، هذا الجدل ربما لم يمنع من أن يتفق الجميع على وجوب الحماية، لكن الخلاف كان في موضعها، فإلى جانب هذين التوجيهين، كان هناك ثمة آراء تجد في القواعد القانونية المدنية والشروط العقدية (تحديدا في حقل المنافسة والأسرار) موضعا مناسبا لحماية حقوق المبرمجين. [2]

في هذه البيئة الجديدة بدأت تظهر التدابير التشريعية في حقل حماية البرمجيات اعتبارا من 1973 (في الفلبين) مع أن موجة هذه التشريعات

---

(1) إعلان طهران، جمشيد ممتاز، مطبوعات الأمم المتحدة (2009). Retrived from،www.un.org/law/avl p.13

(2) Easttom C. Computer Crime Investigation and the Law،New Y press، (2010)، P 33

يتـم إرجاعهـا للثمانينـات لأن الأخـيرة شـهدت تدابـير تشريعيـة وطنيـة واسـعة في حقـل حمايـة البرمجيـات بسـبب الأثـر الـذي تركتـه القواعـد النموذجيـة لحمايـة برامـج الكمبيوتـر الموضوعـة مـن خـبراء المنظمـة العالميـة للملكيـة الفكريـة (الوايبـو) عـام 1978.[1]

وصحيـح أن تشريعـات حمايـة البرامج ترافقـت مع تشريعـات الخصوصية وجرائم الكمبيوتـر، لكنهـا كانـت أسرع تناميـا وأوضـح مـن حيث الـرؤى لمحتوى ولمسـتقبل هذه التشريعـات، ولهـذا فإنهـا أوسـع مـدى من حيـث عددهـا وإذا أردنا أن نعـرف السر فإنه في الحقيقـة يرجـع إلى عاملين أساسـيين،

الأول: وجـود المنظمـة العالميـة للملكيـة الفكريـة (الوايبـو)، التـي سـاهمت عـبر ملتقياتهـا وأدلتهـا الإرشـادية وقوانينهـا النموذجيـة في حسـم الجـدل بشـأن موضـع حمايـة البرمجيـات ليكـون قوانـين حـق المؤلـف لا قوانـين بـراءات الاخـتراع، أي الحمايـة عـبر نظـام الملكيـة الأدبيـة الفكريـة وليـس الملكيـة الصناعيـة الفكريـة.

والثـاني: توجـه سياسـات الأسـواق الرأسـمالية إلى اسـتراتيجيات الاسـتثمار في حقل الملكيـة الفكريـة ومصنفاتهـا كمقدمـة لبنـاء الاقتصـاد الرقمـي الـذي بـدأت أول ملامحـه في اتجـاه الولايـات المتحـدة الأمريكيـة مدفوعـة بتأثير الـشركات متعـددة الجنسـيات لوضـع الملكيـة الفكريـة ضمـن أجنـدة اتفاقيـات تحريـر التجـارة والخدمـات ومسـاومة الولايـات المتحـدة العـالم كلـه عـلى قبـول اتفاقيـات تحريـر التجـارة في البضائـع مقابل إنجـاز تقدم في حقـلي تحريـر الخدمـات والملكيـة الفكريـة.[2]

---

(1) Grabosky، P. Electronic Crime، New Jersey: Prentice Hall، p134 See also McQuade، S. Understanding and Managing Cybercrime، Boston: Allyn & Bacon، (2006) See also Walden، I. Computer Crimes and Digital Investigations، Oxford: Oxford University Press، (2007)

(2) كانـت الولايـات المتحـدة الأمريكيـة مـن بـين الـدول التـي رفضـت الانضـمام لاتفاقيـات الجـات (1947) المتعلقـة بتحريـر التجـارة في البضائـع، وبقـي موقفهـا هـذا واضحـا في جـولات =

وعلى ذلك فإن أكثر تشريعات قانون الكمبيوتر نضجا ووضوحا في أغراضها القوانين أو التدابير التشريعية المتعلقة بحماية الملكية الفكرية لبرامج الكمبيوتر (وفيما بعد قواعد البيانات والدوائر المتكاملة) ويتصور أن تحقق هذه التشريعات أيضا حماية أوسع في السنوات القادمة في حقل أسماء مواقع الإنترنت والمحتوى الرقمي لمواقع الإنترنت.

ولا يعني هذا أن بقية موضوعات تقنية المعلومات لم تحظ بدعم واهتمام هيئات دولية، لكن الفرق أن أيا منها حتى ذلك الوقت لم يكن موضع عمل منظمة متخصصة فيه كما هو حال منظمة الوايبو التي تتولى رعاية الملكية الفكرية وإدارة اتفاقياتها. [1]

وبالتالي فإن مطلع السبعينات شهد الانطلاقة الحقيقة لموجة تشريعات الخصوصية، والسبعينات أيضا (وعلى امتداد الثمانينات والتسعينات) شهد انطلاقة الموجة الثانية المتمثلة بقوانين جرائم الكمبيوتر، في حين شهدت الثمانينات (فعليا) انطلاقة موجة ثالثة من التشريعات المتصلة بالكمبيوتر هي موجة تشريعات حماية البرمجيات التي تمثل المصنف الأهم من بين المصنفات الرقمية ذات الاتصال بالكمبيوتر.

ثلاثة موجات تشريعية: تشريعات الخصوصية (حماية الحق في البيانات الشخصية من مخاطر التكنولوجيا)، قوانين جرائم الكمبيوتر(الاعتداء على نظم المعلومات والمعلومات ببعدها الاقتصادي) وتشريعات حماية برامج الكمبيوتر (الملكية الفكرية). [2]

= المفاوضات التجارية السبعة حتى بدأت جولة الأورغواي (1986 - 1994) والتي شهدت تحولا رئيسا في التجارة الدولية عنوانه قبول أمريكا ضمن تحالف مصالح مع عدد من الدول الصناعية اتفاقيات عديدة في حقل تحرير تجارة البضائع مقابل إدراج اتفاقيات تحرير الخدمات (جاتس) واتفاقية الملكية الفكرية (تربس)، هذا التحول الذي أدى إلى ولادة منظمة التجارة الدولية اعتبارا من 1/1/1995 بموجب إعلان مراكش.

(1) Wall، D.S. Cybercrimes: The transformation of crime in the information age، Cambridge: Polity(2007) P 98

(2) Amitai Etzioni، “The Limits of Privacy”، New York: Basic Books

هـذه حقـول ثلاثـة في سـاحة قانـون الكمبيوتـر، وسـنجد بعـد قليـل أن ثمـة حقل رابـع يـكاد يكـون الوعـاء الـذي يضمهـا جميعـا وهـو حقـل الأعـمال الإلكترونيـة، لكـن يفصـل بـين حقـل الأعـمال الإلكترونيـة والحقـول الثلاثـة، حقـول أخـرى ربمـا لا تكـون مسـتقلة بشـكل كاف في مبناهـا عـن الفـروع القانونيـة التـي تتبعهـا لكنهـا بالتأكيـد خلقـت تغـيرات جوهريـة اسـتلزمتها تقنيـة المعلومـات.

فـأول الحقـول التـي بـرزت عقـب الحقـول الثلاثـة المتقدمـة، قواعـد الإجـراءات الجنائيـة للاسـتدلال والتحقيـق والإثبـات وإجـراءات المحاكمـة المتفقـة مـع طبيعـة الاعتـداءات في الدعـاوى التـي تتعلـق بجرائـم الكمبيوتـر أو الاعتـداء عـلى الخصوصيـة وحتـى في حقـل قرصنـة برمجيـات الحاسـوب المخزنـة داخـل النظـم أو المحملـة مـع الأجهـزة. وبالرغـم مـن أن الـدول الأوروبيـة وأسـتراليا كذلـك قـد تنبهـت لهـذا الموضـوع مبكـرا مـع مطلـع السـبعينات فـإن الموجـة التشريعيـة المتصلـة بهـذه القواعـد بـدأت حقيقـة وعـلى نطـاق واسـع في منتصـف الثمانينـات (ابتـداء مـن عـام 1984 بريطانيـا).[1]

تبـع هـذا الحقـل تدابـير تشريعيـة في ثلاثـة حقـول أخـرى كان للإنترنـت وشـبكات المعلومـات ونمـاء اسـتثمارات الخدمـات التقنيـة الـدور في توجيـه الاهتـمام الحقيقـي بهـا، بـل في ولادة مفهـوم جديـد لبداياتهـا التـي ظهـرت قبـل شـيوع الإنترنـت، فمـع تحـول الإنترنـت إلى الاسـتخدام التجـاري الواسـع، ظهـرت تحديـات قانونيـة جديـدة، بعضهـا ذو اتصـال بتحديـات سـابقة أو قائمـة، كتحديـات حمايـة أمـن المعلومـات في حقـلي الخصوصيـة وجرائـم الكمبيوتـر وحمايـة البرامـج في بيئـة الإنترنـت ذاتهـا، لمـا أتاحتـه مـن تسـهيل ارتـكاب الاعتـداءات بعـد

(2000) p.73. see also United Nations Manual on the Prevention and Control of Computer - Related Crime United Nations Publications 1994

(1) Paul Taylor. Hackers: Crime in the Digital Sublime (Routledge; 1 edition. 1999 ed.). p. 200. See also Yar، M. Cybercrime and Society، London: Sage. (2006)

أن وفرت مدخلا سهلا إلى نظم الكمبيوتر المرتبطة ضمنها. وتحديات أخرى أوجبتها أنماط السلوك الجديدة التي ولدت بولادة الإنترنت، كالبيع والشراء على الشبكات وأداء الخدمة عبر الإنترنت، ومن هذه التحديات التنظيم القانوني للتجارة الإلكترونية.(1)

هذه التحديات التي أوجدها أو ضخمها الإنترنت أو عدل في نطاقها ومخاطرها وجديتها، رافقها موجات تشريعية بدأت في حقل ما يعرف بتنظيم الأمن المعلوماتي والمعايير التقنية وتحديدا ما يتصل بتشفير البيانات، التي انطلقت في عام 1990 من فرنسا تحديدا، ثم في حقل مكافحة المحتوى غير القانوني للمعلوماتية، الذي انطلق عام 1996 في أمريكا. وأخيرا الحقل الأكثر إثارة للجدل وأوسعها تنظيما، حقل الأعمال الإلكترونية الذي اشرنا إليه أعلاه وهو الحقل الرابع المركزي إلى جانب جرائم الكمبيوتر والخصوصية والملكية الفكرية.

وحقل الأعمال الإلكتروني ليس لاحقا للحقول الأخيرة الثلاث، إنما قد نجد تشريعات في إطاره، كالتشريعات المتعلقة بتقنيات الأعمال المصرفية، أو تلك المتعلقة بحجية الإثبات بالوسائل الإلكترونية، سابق بسنوات عديدة للحقول المشار إليها، لكن قولنا بأنه الحقل الأخير زمنيا يرجع إلى تبلور مفاهيم شمولية جديدة في حقل الأعمال الإلكترونية عكسها تحديدا مفهوم التجارة الإلكترونية والبنوك الإلكترونية.(2)

وهذا المفهوم الشامل نجد أنه انطلق مع عام 1996 الذي شهد إقرار

---

(1) Frieden، Jonathan D.; Roche، Sean Patrick "E - Commerce: Legal Issues of the Online Retailer in Virginia".Richmond Journal of Law and Technology 2006 P 13

(2) Graham، Mark "Warped Geographies of Development: The Internet and Theories of Economic Development" (PDF). Geography Compass (2008). P23.

القانون النموذجي للتجارة الإلكترونية من قبل لجنة الأمم المتحدة لقانون التجارة (اليونسترال).[1]

وسنجد أن دولا على المستوى التشريعي كانت قد بدأت الاهتمام بمسائل الأعمال الإلكترونية:

(كالإثبات بالوسائل الإلكترونية، وحجية مستخرجات الحاسوب، والتنظيم القانوني لبطاقات الائتمان وغيرها) وذلك في أواخر السبعينات وبداية الثمانينات،[2] لكنها لم تكن ضمن التصور الشامل للتجارة الإلكترونية التي ارتبطت واقعا بأنشطة الاستثمار على الإنترنت.[3]

أما من حيث الأطر الدولية العاملة في ميادين الموضوعات المتقدمة، فإننا سنجد الجهد الأساسي والمميز موزع بين منظمة التعاون الاقتصادي والتنمية وهيئات أوروبا (مجلس أوروبا والمفوضية الأوروبية واتحاد أوروبا والبرلمان الأوروبي) والأمم المتحدة، ومجموعة الدول الصناعية الثمانية، والوايبو، والإنتربول، ومنظمة التجارة الدولية وغيرها من المنظمات.[4]

الخصوصية، جرائم الكمبيوتر، الملكية الفكرية للمصنفات الرقمية، الإجراءات الجنائية في البيئة الرقمية، المعايير والمواصفات والأطر التنظيمية للتقنية وتأثيرها على النشاط الإداري والخدمي، المحتوى غير القانوني للمعلوماتية، الأعمال الإلكترونية وتحديدا التجارة الإلكترونية، وفي إطار

(1) L. Castellani، 'The United Nations Electronic Communications Convention - Policy Goals and Potential Benefits'، Korean Journal of International Trade & Business Law 1 (2010) P49 See also

(2) Jonathan D. Frieden and Leigh M. Murray، The Admissibility of Electronic Evidence Under the Federal Rules of Evidence، XVII Rich. J.L. & Tech. (2011(P 78

(3) Daniel J. Ryan; Gal Shpantzer."Legal Aspects of Digital Forensics". (August 2010) p.83.

(4) Etzioni، A. "Are new technologies the enemy of privacy"، (2007) p.69.

كل منهما ثمة تشريعات ومجهودات دولية وإقليمية وسياسات واستراتيجيات ومحتوى ومشكلات أيضا.[1]

هذه الحقول والموجات التشريعية - وان كانت سبعة وفق التوصيف المتقدم أربعة منها تكاد تستقل تماما في أطرها التنظيمية والتشريعية - إلا أن كل منها شهد تطورا فتفرع في إطارها أيضا حقول أخرى، بعضها يرتبط بغيره وبعضها يستقل في موضعه عنها، لكن حركة التطور يأخذها شيئا فشيئا نحو التكاملية والتوحد في إطار واحد، وهذا ما سيؤدي إلى تبلور قانون الكمبيوتر كفرع مستقل عن بقية الفروع القانونية.[2]

ولو أعدنا حصر كافة القطاعات المتقدمة وما تفرع عنها سوف يتم التوصل إلى الحقول التشريعية التالية في نطاق قانون الكمبيوتر:

1. تشريعات الخصوصية أو قواعد حماية تجميع ومعالجة وتخزين وتبادل البيانات الشخصية.

2. تشريعات جرائم الكمبيوتر، ومن ثم تطورها لتشمل جرائم الإنترنت وشبكات الاتصال ضمن مفهوم أشمل (أمن المعلومات) وفي نطاق الاعتراف للمعلومات بالحماية القانونية من كافة الأنشطة التي يكون الكمبيوترات فيها هدفا أو وسيلة أو بيئة للجريمة.

3. تشريعات الملكية الفكرية في حقل حماية البرمجيات ومن ثم تطورها لتشمل بقية المصنفات الرقمية، إلى جانب تطورها على نحو يعكس الاتجاهات العالمية في إدراج الملكية الفكرية ضمن تنظيمات التجارة الدولية للتوجه الحاصل نحو الاقتصاد الرقمي والاقتصاد المؤسس على المعرفة ونحو رأس المال الفكري.

---

(1) يونس عرب والتدابير التشريعية العربية لحماية المعلومات والمصنفات الرقمية،ورقة عمل مقدمة أمام: الندورة العلمية الخامسة حول دور التوثيق والمعلومات في بناء المجتمع العربي – النادي العربي للمعلومات – دمشق،2013 ص52

(2) جينشار وآخرين، الإنترنت والقانون، منشورات مون كريستان، باريس 1999 ص133

4. تشريعات الأصول الإجرائية الجزائية، وتشريعات الإثبات المتفقة مع عصر الكمبيوتر والمعلومات والتي هي في الحقيقة تطوير لقواعد الإجراءات والإثبات، لكنها أيضا تتصل عضويا بالحقوق الجديدة المعترف بها في ميدان تقنية المعلومات.

5. تشريعات المحتوى الضار:(الحماية من محتوى المعلوماتية على الإنترنت)، ثمة اتجاهات متباينة بين توجه لدمجها مع تشريعات أمن المعلومات كما في أوروبا، أو استقلالها عنها كما في أمريكا.

6. تشريعات معايير الأمن المعلوماتي وتطورها إلى تشريعات المواصفات القياسية لتبادل البيانات والتشفير، وثمة أيضا اتجاهات لاعتبارها جزءا من تشريعات التجارة الإلكترونية في حين هناك اتجاهات لتناول كل موضوع من مواضيعها في تشريع مستقل.

7. التشريعات المالية والمصرفية فيما يتصل بالمال الإلكتروني وتقنيات الخدمات المصرفية والمالية وفي مقدمتها البطاقات المالية ونظم التحويل الإلكتروني والتي تطورت لتشمل أطرا جديدة في حقل التوجه نحو الأتمتة الكاملة للعمل المصرفي والمالي (البنوك الإلكترونية).

8. تشريعات الاستثمار والتجارة والضرائب والجمارك والاتصالات والأنظمة الحكومية المرتبطة بالمشروعات التقنية أو المتأثرة بتقنية المعلومات.

9. تشريعات التجارة الإلكترونية:(التواقيع الإلكترونية، والتعاقد الإلكتروني، والتسوق الإلكتروني)، وهذه الطائفة تتضمن قواعد تتصل بكافة حقول تقنية المعلومات لأنها أثارت تحديات فيها جميعا، لهذا ثمة حقيقة أن التجارة الإلكترونية وحدها برغم كونها

آخر حلقات تقنية المعلومات في الوقت الراهن فإنها الإطار الأوسع المؤهل لتوحيد قواعد قانون الكمبيوتر.

10. تشريعات (اتفاقيات ومعاهدات) الاختصاص والقانون المطبق على المنازعات القضائية في بيئة الإنترنت (بشكل خاص منازعات الملكية الفكرية ومنازعات التجارة والأعمال والبنوك الإلكترونية).

الفرع الثالث

خصائص ومحتوى تشريعات الخصوصية البيانات

إن المصالح المتعين حمايتها والحقوق المتعين الاعتراف بها في بيئة تقنية المعلومات تتوزع بين حق الكافة في الحصول على المعلومات، والحقوق والمصالح والمكنات المقررة لحائز أو صاحب المعلومة أو النظام التقني أو صاحب الإبداع أو مستثمر الابتكار وفق الحال، وحقوق المستهلك، وحقوق المجتمع.

وهذه المصالح وما يتفرع عنها تتطلب إحداث توازن بين استخدام التقنية والتحكم بها وبين حقوق الأفراد والمجتمع ومصالحهما، هذا التوازن هو ما يتحول إلى قواعد قانونية تضمها أحكام قوانين تقنية المعلومات في فروعه المختلفة[1]، فإذا ما أردنا تحويلها لقواعد (عملية) تتصل بالمعلومات للانطلاق نحو رسم ملامح النظرية العامة للمعلومات فإننا نكون أمام الأسس العامة التالية (المتعين إقرارها في النظام القانوني):

1. إن الفرد من حيث الأصل له الحق في الحصول على المعلومات، وتظل الحقائق والأفكار العامة ملكا شائعا للبشرية لا ترد عليها مكنات قانونية تحد من الإفادة منها ولا سلطات استئثارية إلا متى ما اتصلت بجهد خلقي (ليس هو دائما المفهوم المقرر في نظام الملكية الفكرية فحسب) يبرر الإقرار بمصالح وحقوق ترتبط بصاحب الجهد الخلقي المتصل بها. فالأفكار حول تصميم موقع

(1) Richard A. Posner، The Economics of Privacy،The American Economic Review،Vol. 71، No.)2)، Papers and Proceedings of the Ninety - Third Annual Meeting of the American Economic،Association (May، 1981)، pp. 405 - 409

الإنترنت تظل أفكارا شائعة لا يستأثر بملكيتها أحد، لكن متى ما تحولت إلى أنماط خلقها مصمم موقع ما كانت ملكا في إطارها الإبداعي هذا للشخص الذي ابتكرها، والخوارزميات المستخدمة في البرمجيات لا يدعي ملكيتها أحد، لكن ورودها ضمن تبويب معين ينتج برنامجا مبتكرا تخلق للشخص الذي قام بذلك مكنة الاعتراف بحقه في نسبة هذا الإبداع له وفي حماية استغلاله المادي.

2. إن المعلومات تعد مالا، ومن ثم يجب أن تشمل بالحماية التي تتوفر للأموال ومستجداته.[1]

3. المعلومات لها ذات القيمة الاقتصادية للأموال وربما تفوقها في ظل العصر الذي نعيشه.

4. إن تتساوى التصرفات التي تتم في البيئة الرقمية مع مثيلتها في البيئة المادية.

5. إن توفر الحماية الجنائية مماثلة لما يتم في البيئة المادية.

6. توفير البيئة اللازمة للتطبيق من الناحية الإجرائية والضبط والتفتيش.[2]

ومن ثم يرى الباحث أن التالي هو مضمون خصائص ومحتوى تشريعات الخصوصية بوجه عام:

1. مسماها الشائع:

قوانين الخصوصيةPrivacy أو قوانين حماية المعطياتData Protection laws.

(1) Levin، Richard C. and Mark B. Myers. A Patent System for the 21st Century. Washington، D.C.: The National Academies Press(2004).P 109

(2) Witten، Ian H.; Frank، Eibe; Hall، Mark A. Data Mining: Practical Machine Learning Tools and Techniques (3 ed.). Elsevier 2011). P 30

2. وصفها العام:

تشريعات حماية الحياة الخاصة من مخاطر المعالجة الإلكترونية للبيانات الشخصية.

3. مبرر وجودها:

هذه التشريعات جاءت كرد فعل للتحديات التي واجهتها الحياة الخاصة بسبب مخاطر المعالجة الآلية للبيانات الشخصية وازدياد أنشطة جمع (Collecting) وتخزين (Storing) وتبادل ونقل البيانات (Transmitting data) بالتقنيات الحديثة.

4. هدفها ونطاقها:

سنت هذه القوانين لحماية حق المواطنين في الخصوصية وحماية بياناتهم الخاصة وأسرارهم ضمن قواعد إدارية ومدنية وجزائية.

5. الحقبة الزمنية لانطلاقها وترتيبها بين موجات تشريعات التقنية:

في عام 1968 وعلى أثر عقد مؤتمر الأمم المتحدة (طهران) لحقوق الإنسان ومناقشة موضوع مخاطر تكنولوجيا المعلومات على الحق في الخصوصية ظهرت هذه التشريعات كأول موجة تشريعية وقد انطلقت خلال السبعينات والثمانينات. وخضعت لتعديلات متتالية خلال الثمانينات والتسعينات.

6. الفرع القانوني ذو العلاقة:

حقوق الإنسان (تحديدا الحق في الحياة الخاصة)، والقانون الجنائي (المسؤولية الجزائية عن الإخلال بواجبات المعالجة وعن إفشاء البيانات)، القانون الإداري (أنظمة التنظيم الإداري، وقواعد نقل تبادل المعلومات بين الهيئات الحكومية).

7. محلها ذو العلاقة بالتكنولوجيا:

البيانات الشخصية المخزنة والمعالجة والمتبادلة بواسطة الكمبيوتر وشبكات نقل المعلومات (بما فيها وفي مقدمتها الإنترنت).

8. محتواها بوجه عام:

القواعد القانونية المنظمة لمعالجة البيانات وتخزينها في بنوك المعلومات وتبادلها وتشمل القواعد التي تحظر جمع المعلومات دون سند قانوني وتوجب جمعها للغرض المعلن واستخدامها في هذا الغرض وحده، وتتيح الحق في تصحيحها وتعديلها من أصحابها، ولا تجيز إفشاءها وتقرر عقوبات على القائمين بالمعالجة والتحكم في هذه البيانات عند الإخلال بواجباتهم وتقييم المسؤولية على التوصل إليها من الأشخاص الخارجين عن المؤسسة المعنية بالجمع والمعالجة والمسؤولية عن إفشائها أو الابتزاز بواسطتها.

المطلب الثاني

الأنماط والنماذج التشريعية في حقل حماية البيانات

إن خصوصية البيانات أو قوانين حماية البيانات تمنع إفشاء البيانات الشخصية المتعلقة بالأفراد أو إساءة استخدامها، إن أكثر من ثمانين دولة على مستوى العالم قامت بتشريع قوانين كاملة للخصوصية فمثلا في أغلبية الدول الأوروبية وكذلك دول أمريكا اللاتينية بالإضافة إلى دول من آسيا وأفريقيا.[1]

قوانين الخصوصية الدولية International Privacy Laws

هناك قوانين دولية مختلفة والتي تحمي حقوق الخصوصية. فعلى سبيل المثال: يحتوى الميثاق الدولي حول الحقوق المدنية والسياسية International Covenant on Civil& Political Rights لسنة 1966 حق عام للخصوصية والذي يحمي مجالات مثل: عائلة ومنزل ومراسلات وسمعة الفرد في حين أن ميثاق الأمم المتحدة حول حقوق الطفل United Nations Convention on the Right of the Child والإعلان العالمي لحقوق الإنسان the Universal Declaration of Human Rights سبل حماية مماثلة للخصوصية.

ولقد شهدت منظمة الاقتصاد والتعاون والتنمية Organization for Economic، Cooperation & Development حول حماية الخصوصية وتدفق البيانات الشخصية عبر الحدود بداية قانون الخصوصية الفيدرالي Federal Privacy Act لسنة 1988.

(1) Greenleaf، Graham. "Global Data Privacy Laws: 89 Countries، and Accelerating". Social Science Electronic Publishing، Inc. Retrieved 16 February (2014) p.114.

ولكثير من الدول قوانين للخصوصية ذات طبيعة مماثلة لحماية المعلومات.

وسنعرض لنماذج من تشريعات خصوصية البيانات في عدة دول منها :

- الولايات المتحدة **(الفرع الأول)**.
- كندا **(الفرع الثاني)**.
- وأوروبا **(الفرع الثالث)**.
- ثم قوانين خصوصية البيانات في سويسرا**(الفرع الرابع)**.
- وأخيراً خصوصية البيانات في أستراليا**(الفرع الخامس)**.

الفرع الأول

خصوصية البيانات في الولايات المتحدة

ومـن الملاحـظ أن الولايـات المتحـدة الأمريكيـة لم تعتمـد قوانـين شـامله لحمايـة خصوصيـة البيانـات بـل اعتمـدت عـلى القوانـين القطاعيـة المتعلقـة بـكل قطـاع عـلى حـدة وذلـك في بعـض المناطـق.

هـذه الحزمـة مـن القوانـين شرعـت عـلى أسـاس الاسـتخدام العـادل للبيانـات الشـخصية، وفي عـام 1970 قامـت إدارة الصحـة والتعليـم بالولايـات المتحـدة بطـرح أول هـذه القوانـين معتمـدة عـلى بعـض المبـادئ الأساسـية في حمايـة البيانـات الشـخصية ومنهـا:

- أن يكـون جمـع البيانات لغرض محدد.
- البيانـات الشـخصية التـي يتـم الحصـول عليهـا لا يجـوز التصريـح بهـا لأي فـرد أو مؤسسـه إلا برضـاء صاحـب البيانـات أو بسـند قانـوني.
- جميـع البيانـات المجمعـة من الأفراد يجب أن تكـون دقيقه ومحدثه.
- لابـد مـن وجـود آليـة تمكـن الأفراد مـن مراجعـة بياناتهـم الشـخصية لضمان الدقـة، بالإضافـة إلى التمكـن مـن الحصـول عـلى تقاريـر دوريـة.
- يجـب مسـح البيانات الشـخصية في حاله انتهاء الغرض مـن تجميعها.
- يحظـر نقـل البيانـات إلى المواقـع غـير الآمنـة عـلى مثلهـا مـن البيانـات ا لشـخصية .
- بعـض البيانـات قـد تكـون حساسـة حيـث إن الإفصـاح عنهـا لا يكـون إلا في الحـالات القصـوى وذلـك مثـل (الديـن والتوجـه الجنـسي).[1]

(1) Paul M. Schwartz Privacy، Information، and Technology، Aspen Publishers، (2006)، pp. 9-11

الفرع الثاني

خصوصية البيانات في كندا

أما كندا فقد وضعت قانون حماية المعلومات الشخصية والمستندات الإلكترونية وعرفت فيه البيانات أو "المعلومات الشخصية" بشكل دقيق على أنها هي المعلومات التي تخص فرد محدد ولكنها لا تشمل الاسم أو اللقب أو عنوان العمل أو رقم هاتف موظف في هيئة أو مؤسسة.

وكذلك وضع القانون تعريف للهيئة التي تستغل المعلومات أو البيانات الشخصية بأنها "الهيئة" - وتعني جمعية أو شراكة أو شخص أو اتحاد تجاري وحددت الأعمال التي يتم استغلال البيانات بصددها موضحا أنها "الأعمال أو التعهدات أو التجارة الفيدرالية" - وتعنى أي عمل أو تعهد يقع ضمن السلطة التشريعية للبرلمان ويشمل:

1. عمل أو تعهد أو تجارة تجري أو تستمر أو تكون مرتبطة بالملاحة والشحن سواء كانت برية أو بحرية بما في ذلك تشغيل السفن والنقل باستخدام السفن لأي مكان في كندا.
2. سكة حديدية أو قناة أو تلغراف أو أي عمل أو تعهد آخر يربط إحدى المقاطعات بمقاطعة أخرى أو التي تمتد لما يتعدى حدود المقاطعة.
3. خط ملاحي يربط إحدى المقاطعات بمقاطعة أخرى أو يمتد لما يتعدى حدود المقاطعة.

---

see also Mena، Jesús (2011). Machine Learning Forensics for Law Enforcement، Security، and Intelligence. Boca Raton، FL: CRC Press (Taylor & Francis Group).2010

4. ناقلة بحرية بين إحدى المقاطعات ومقاطعة أخرى أو مقاطعة ودولة أخرى غير كندا.

5. المطارات أو الطائرات أو خطوط النقل الجوي.

6. محطة بث إذاعي

7. بنك

8. عمل برغم أنه يقع كلية داخل المقاطعة إلا أن البرلمان يعلن قبل أو بعد تنفيذه أنه موجه للمصلحة العامة لكندا أو لمصلحة مقاطعتين أو أكثر من المقاطعات الكندية.

9. عمل أو تعهد أو تجارة خارج السلطة التشريعية الحصرية لتشريعات المقاطعات.

10. عمل أو تعهد أو تجارة ينطبق عليه القوانين الفيدرالية في إطار معنى القسم الثاني من قانون الأوقيانيوس Oceans، وفقا للقسم العشرين من ذلك القانون ووفقا لأي لوائح تصدر تحت الفقرة رقم 26 (1)(ك) من ذلك القانون.[1]

ويمنح قانون حماية المعلومات الشخصية والمستندات الإلكترونية الكندي الأفراد الحق في:

فهم الأسباب التي تدعو الهيئات إلى جمع أو استخدام أو الإفصاح عن المعلومات الشخصية، ترقب قيام الهيئات بجمع أو استخدام أو الإفصاح عن المعلومات الشخصية بشكل مناسب وملائم، هم من لدى الهيئة يتحمل مسؤولية حماية المعلومات الشخصية للأفراد، ترقب أن تقوم الهيئات بحماية المعلومات الشخصية بشكل مناسب وآمن، ترقب أن تكون المعلومات

(1) Iris Fischer، Nicole Henderson. "Ontario Court of Appeal Recognizes New Privacy Tort". Blake، Cassels & Graydon، 2003، P 69

الشخصية الموجودة بحوزة الهيئات دقيقة وكاملة ومحدثة وكذلك أن تتاح للأفراد الدخول على معلوماتهم الشخصية وطلب القيام بأي تصحيحات أو أن يكون للأفراد الحق في تقديم شكوى ضد الهيئات.[1]

يطالب قانون حماية المعلومات الشخصية والمستندات الإلكترونية الهيئات بـ:

الحصول على الموافقة قبل جمع واستخدام والإفصاح عن المعلومات الشخصية، بجمع المعلومات الشخصية بشكل مناسب وملائم وقانوني، بالإضافة إلى وضع سياسات للمعلومات الشخصية تكون واضحة وجاهزة لحماية المعلومات الشخصية للأفراد.

تم تفعيل قانون الخصوصية في الأول من يوليو عام 1983. ويفرض هذا القانون التزامات على نحو 250 إدارة ووكالة حكومية فيدرالية احترام حقوق الخصوصية بتقييد عمليات الجمع والاستخدام والإفصاح عن المعلومات الشخصية. ويعطي قانون الخصوصية للأفراد حق الدخول على المعلومات الشخصية الخاصة بهم، وطلب تصحيحها من قبل تلك الهيئات الحكومية الفيدرالية.[2]

كما أن للأفراد أيضا قانون حماية المعلومات الشخصية والمستندات الإلكترونية والذي يضع قواعد أساسية حول الكيفية التي يمكن بها لهيئات القطاع الخاص جمع واستخدام والإفصاح عن المعلومات الشخصية في إطار الأنشطة التجارية.

ويمنح القانون الأفراد حق الدخول على المعلومات الشخصية التي قد تكون هذه الهيئات قدمت بجمعها عنهم وطلب تصحيحها.

---

(1) "An Act respecting the protection of personal information in the private sector".. publicationsduquebec.gouv.qc.ca. 2012

(2) Rob Barrass، Lyndsay A. Wasser،"Seclusion intrusion: a common law tort for invasion of privacy". McMillan LLP،(2012) p.46.

في البداية، تم تطبيق قانون حماية المعلومات الشخصية والمستندات الإلكترونية على المعلومات الشخصية للعملاء والموظفين والتي تم جمعها أو استخدامها أو الإفصاح عنها في إطار الأنشطة التجارية من قبل القطاع الخاص الذي تنظمه القوانين الفيدرالية وهيئات مثل البنوك وخطوط الطيران وشركات الاتصالات.

وينطبق القانون الآن على المعلومات الشخصية التي تم جمعها أو استخدامها أو الإفصاح عنها من قبل قطاع مبيعات التجزئة وشركات النشر وصناعة الخدمات والمصنعون والهيئات الأخرى التي تخضع للنظم الإقليمية. ولا ينطبق القانون على المعلومات الشخصية لموظفي هذه الهيئات التي تخضع للنظم الإقليمية.[1]

وقد تعفي الحكومة الفيدرالية الهيئات أو الأنشطة القائمة في الأقاليم التي قوانين الخصوصية الخاصة بها إذا ما كانت متماثلة بشكل جوهري مع القانون الفيدرالي.

ولسوف يستمر تطبيق قانون حماية المعلومات الشخصية والمستندات الإلكترونية في تلك الأقاليم على القطاع الخاص الذي يخضع للقوانين الفيدرالية وعلى المعلومات الشخصية في المعاملات المتبادلة داخل الأقاليم، والمعاملات الدولية من قبل كافة الهيئات المشاركة في الأنشطة التجارية.

وتقع عملية الإشراف على القانونين الفيدراليين على عاتق مفوض الخصوصية الكندي، والذي يتمتع بصلاحية تلقي الشكاوى والتحري عنها.

---

(1) Marco،P.M"Personal Health Information Custodians in New Brunswick Exemption Order:". Department of Justice. 2011 p 31 see also Personal Information Protection and Electronic Documents Act، Published by the Minister of Justice at the following address:،http://laws - lois. justice.gc.ca retrived 12 - 6 - 2014

ولـكل إقليـم ومقاطعـة تشريـع الخصوصيـة الـذي ينظـم عمليـة جمع واسـتخدام والإفصـاح عـن المعلومـات الشـخصية التـي تحتفـظ بهـا الـوكالات الحكوميـة.

وهـذه القوانـين تـزود الأفـراد بحقـوق عامـة تتيح لهـم الدخـول عـلى معلوماتهم الشـخصية وتصحيحهـا، وتتـم عمليـة الإشراف مـن خـلال إمـا مفـوض مسـتقل أو أمـين المظـالم ombudsman المخـول بتلقـي الشـكاوى والبحـث فيهـا.

وبالنسـبة للقطـاع الخـاص فينطبـق قانـون حمايـة المعلومـات الشـخصية والمسـتندات الإلكترونيـة عـلى جميـع الهيئـات المشـاركة في الأنشـطة التجاريـة مـا لم تعفـي الحكومـة الفيدراليـة إحـدى الهيئـات أو أحـد الأنشـطة في الإقليـم مـما يكـون لديهـا / لديـه تشريـع أسـاسي مماثـل للقانـون.[1]

---

(1) Perun، Halyna; Michael Orr، Fannie Dimitriadis (2005). "2". Guide to the Ontario Personal Health Information Protection Act. Toronto ON، Canada: Irwin Law. pp. 19–20.. Cite uses deprecated parameters (help)

الفرع الثالث

خصوصية البيانات في أوروبا

قد نظمت أوروبا قوانين خصوصية البيانات سواء على مستوى الاتحاد الأوروبي(أولاً) أو كل دولة على حدة مثل فرنسا (ثانياً) والمملكة المتحدة (ثالثاً).

أولاً: الاتحاد الأوروبي.

أما في أوروبا فيتم تنظيم وتنفيذ حق خصوصية البيانات بشكل كبير وفعال. وتنص المادة رقم 8 من المعاهدة الأوروبية لحقوق الإنسان European Convention on Human Rights على حق احترام الحياة الشخصية والعائلية للفرد ومنزله ومراسلاته وفقا لقيود محددة.

ولقد أعطت المحكمة الأوروبية لحقوق الإنسان European Court of Human Rights لهذه المادة تفسيرا متسعا في قانونها Jurisprudence. فوفقا لقانون المحكمة للأحوال Court's case law، فإن قيام المسؤولين الحكوميين بجمع المعلومات حول فرد دون الحصول على موافقته عادة ما تقع ضمن مجال المادة رقم 8.

وبذلك، فإن جمع المعلومات لأجل التعداد السكاني أو تسجيل بصمات اليد والصور في سجل الشرطة أو جمع بيانات طبية أو تفصيلات حول المصروفات الشخصية وتنفيذ نظام تحديد الشخصية قد أثارت الكثير من القضايا المتعلقة بخصوصية البيانات.[1]

(1) Pieter van Dijk،Godefridus J. H. Hoof،G. J. H. Van Hoof "Theory and Practice of the European Convention on Human Rights"و Martinus Nijhoff Publishers، (1998) P.136

ولا تقبل المحكمة أي تدخل للدولة في خصوصية الأفراد إلا بتوافر ثلاثة شروط هي:

1. إذا كان التدخل وفقا للقانون.
2. إذا كان التدخل يتلمس هدفا مشروعا.
3. إذا كان التدخل ضروريا في مجتمع ديمقراطي.

ولا تعد الحكومة بالكيان الوحيد الذي قد يفرض تهديدا على خصوصية البيانات، فالمواطنون الآخرون والشركات الخاصة تحديدا يشتركون في أنشطة تشكل تهديدا أكبر خاصة مع انتشار المعالجة الإلكترونية للبيانات. ولقد تم إبرام معاهدة حماية الأفراد المتعلقة بالمعالجة الآلية للبيانات الشخصية Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data داخل المجلس الأوروبي في عام 1981. وتلزم هذه المعاهدة الموقعين عليها بسن التشريعات المتعلقة بالمعالجة الآلية للبيانات الشخصية وهو ما قامت كثير من الدول بعمله بالفعل.[1]

وحيث إن جميع الدول الأعضاء في الاتحاد الأوروبي من الموقعين على المعاهدة الأوروبية لحقوق الإنسان ومعاهدة حماية الأفراد المتعلقة بالمعالجة الآلية للبيانات الشخصية، كانت المفوضية الأوروبية European Commission مهتمة بأن تشريعات حماية البيانات المتباينة سوف تبرز وتعيق التدفق الحر للبيانات داخل إقليم الاتحاد الأوروبي. لذلك، قررت المفوضية الأوروبية التقدم باقتراح لتوفيق قانون حماية البيانات داخل الاتحاد الأوروبي. ولقد قام البرلمان الأوروبي ووزارات الحكومات القومية بتطبيق

(1) Explanatory Report on the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Dat، Council of Europe،Startsbourg (1981) P.29

توجيه حماية البيانات Data Protection Directive في عام 1995 وكان لزاما أن يتم نقله إلى القانون الوطني مع نهاية عام 1998.[1]

وهنا نبذه عن التوجيه الأوروبي بشأن حماية البيانات والذي سوف يتم تناوله بالبحث المفصل لاحقا.

يحتوى التوجيه على عدد من المبادئ الأساسية والتي يتوجب على الدول الأعضاء الالتزام بها. وعلى أي شخص يقوم بمعالجة البيانات الشخصية أن يلتزم بمبادئ الممارسة الجيدة الثمانية الواجبة التنفيذ[2]. وتحدد هذه المبادئ إلى أن البيانات يجب أن:

1. يتم معالجتها بشكل عادل وقانوني.
2. يتم معالجتها لأغراض محدودة.
3. تكون المعالجة مناسبة ومعنية وغير مفرط فيها.
4. تكون المعالجة دقيقة
5. لا يتم الاحتفاظ بها فترة أطول مما هو ضروري.
6. يتم معالجتها وفقا لحقوق صاحب البيانات.
7. تكون مؤمنة.
8. يتم نقلها فقط إلى الدول التي تتوافر لديها الحماية المناسبة.

---

(1) William J. Clinton & Albert Gore، Jr.، A Framework for Global Electronic Commerce، July 1، 1997، available at http://www.technology.gov/digeconomy/framewrk.htm; See also Robert R. Schriver، You Cheated، You Lied: the Safe Harbor Agreement and Its Enforcement By the Federal Trade Commission، 70 Fordham L (2002)

(2) European Commission - Protection of personal dataavailable at http://ec.europa.eu/justice/data - protection/index_en.htm P.53

وتغطي البيانات الشخصية كلا من الحقائق والآراء الخاصة بالفرد. كما أنها تشمل أيضا معلومات متعلقة بنوايا مراقب البيانات Data Controller[1] تجاه الفرد برغم أن سوف يتم تطبيق بعض الاستثناءات الظرفية المحدودة. أما فيما يتعلق بمفهوم المعالجة، فإن تعريف المعالجة أصبح أكثر اتساعا عن ذي قبل. فعلى سبيل المثال، تتضمن المعالجة مفاهيم "الحصول" و"الاحتفاظ" و"الإفصاح"[2].

ولقد قامت جميع الدول الأعضاء في الاتحاد الأوروبي بتطبيق تشريع متسق مع هذا التوجيه أو قامت بتكييف قوانينها القائمة. كما أن لدى كل دولة سلطتها الإشرافية الخاصة بها لمراقبة مستوى الحماية.

ونتيجة لذلك، فإن نقل المعلومات الشخصية - من الناحية النظرية - من الاتحاد الأوروبي إلى الولايات المتحدة يعد محظورا عندما لا تتوافر سبل حماية الخصوصية المناظرة في الولايات المتحدة.

وعلى الشركات الأمريكية التي تسعى للتعامل مع بيانات الاتحاد الأوروبي أن تلتزم بإطار الملاذ الآمن Safe Harbour. والمبادئ الرئيسة للبيانات التي يتم حمايتها وهي محدودية عملية جمع البيانات وموافقة الفرد والدقة والتكامل والأمن وحق الفرد في مراجعة البيانات وحذف ما يراه منها.

ونتيجة لذلك، فإن لعملاء الهيئات الدولية مثل أمازون Amazon "وإي باي" eBay بالاتحاد الأوروبي القدرة على مراجعة وحذف المعلومات

---

(1) According to the Data Protection Principals the Data Controller means ... a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are، or are to be، processed.

(2) Data Protection،Where does processing occur?، "International Business Trade and Taxation" (March 2014) P.72

في حـين لا يتيـسر هـذا الأمـر للأمريكيـين. وفي الولايـات المتحـدة، نجـد أن الفلسـفة التوجيهيـة المناظـرة هــي قانـون الاسـتخدام العـادل للمعلومـات Code of Fair Information Practice

واختـلاف اللغـة هنـا لـه أهميتـه: ففـي الولايـات المتحدةيـدور الجـدال حـول الخصوصيـة في حـين أن الجـدال في الاتحـاد الأوروبي يـدور حـول حمايـة البيانـات. ويـرى بعـض الفلاسـفة أن تحريـك الجـدال مـن الخصوصيـة إلى حمايـة البيانـات يبـدو كآليـة للانتقـال إلى الأمـام في الواقـع العمـلي في وقـت لا يحتاج إلى اتفاق حول الأسـئلة الرئيسـة المتعلقـة بطبيعـة الخصوصيـة.

ثانياً: في فرنسـا.

قامـت فرنسـا بتطبيـق قانونهـا القائـم رقـم 78 - 17 الصـادر في 6 ينايـر 1978 والمتعلـق بتكنولوجيـا المعلومـات والملفـات والحريـات المدنيـة[1].

ثالثاً:المملكـة المتحدة:

في المملكـة المتحـدة، قـام قانـون حمايـة البيانـات 1998 (مفـوض المعلومـات) Data Protection Act 1998 (Information Commissioner) بتطبيـق التوجيـه المعنـي بحمايـة البيانـات الشـخصية[2] وهـو يحـل محـل قانـون حمايـة البيانـات الصـادر في Data Protection Act 1984. وسـوف نتنـاول بالتفصيـل تاريـخ القوانـين التـي تحمـي الخصوصيـة في المملكـة المتحـدة لاحقـا

أمـــا في مقاطعـــات كولومبيـــا البريطانيـــة British Columbia وألبرتـــا Alberta والكويبـــك فتعـــد Quebec هـــي المقاطعـــات الوحيـــدة التـــي تطبـــق

(1) http://www.cnil.fr/ retrived 22/5/2013

(2) Guide to data protection retrived from Information Commissioner›s Office - ICOhttp://ico.org.uk/for_organisations/data_protection 2/5/2013 P.10

قوانـين معـترف بأنهـا تتماثـل تماثـلا كبـيرا مـع قانـون حمايـة المعلومـات الشـخصية والمسـتندات الإلكترونيـة.

وتنظـم هـذه القوانـين قيـام الـشركات وغيرهـا مـن الهيئـات بجمـع واسـتخدام والإفصـاح عـن المعلومـات الشـخصية وتمنـح الأفـراد حقـا عاما بالدخـول عـلى معلوماتهم الشـخصية وتصحيحهـا. وفي الوقـت ذاتـه، قامـت كل مـن مقاطعـات أونتاريـو Ontario ونيـو برنزويـك New Brunswick ونيـو فاوندلاند Newfoundland ولابرادور Labra- dor بتطبيـق تشريـع لحمايـة معلومـات الصحـة الشـخصية والـذي تـم إقـراره بأنـه مـن القوانـين المماثلة بشـكل أسـاسي[1].

---

(1) Rob Barrass، Lyndsay A. Wasser،"Seclusion intrusion: a common law tort for invasion of privacy".McMillan LLP. (2012). P. 113

الفرع الرابع

خصوصية البيانات في سويسرا

في حين أن سويسرا ليست عضوا في الاتحاد الأوروبي أو في المنطقة الاقتصادية الأوروبية European Economic Area، فقد قامت جزئيا في عام 2006 بتنفيذ توجيه الاتحاد الأوروبي المعني بحماية البيانات الشخصية وذلك بالانضمام إلى اتفاقية تأمين المعدات الطرفية Secure Terminal Equipment (STE 108) للمجلس الأوروبي وللتعديل المقابل للقانون الفيدرالي لحماية البيانات. ومع ذلك، يفرض القانون السويسري قيودا أقل على معالجة البيانات عما يوجبه التوجيه في جوانب عدة.

في سويسرا، تضمنت المادة 13 من الدستور الفيدرالي السويسري Swiss Federal Constitution الحق في الخصوصية. ولقد وضع القانون الفيدرالي السويسري لحماية البيانات[1] والمرسوم الفيدرالي السويسري لحماية البيانات Swiss Federal Data Protection Ordinance موضع التنفيذ في الأول من يوليو 1993.

كما وضعت أحدث التعديلات على القانون الفيدرالي السويسري لحماية البيانات والمرسوم الفيدرالي السويسري لحماية البيانات موضوع التنفيذ في الأول من يناير 2008.

وينطبق القانون الفدرالي السويسري لحماية البيانات على قيام الأفراد والوكالات الحكومية الفيدرالية بمعالجة البيانات الشخصية. وعلى نقيض تشريعات حماية البيانات لكثير من الدول الأخرى، يقوم القانون الفيدرالي

(1) Swiss Federal Data Protection Act (DPA).P.52 available at http://www.edoeb.admin.ch/org/00129/index.html?langen

السويسري لحماية البيانات بحماية كل من البيانات الشخصية المتعلقة بالأشخاص الطبيعيين وكذلك الكيانات القانونية.[1]

ويقوم المفوض الفيدرالي السويسري لحماية البيانات والمعلومات تحديدا بالإشراف على التزام الوكالات الحكومية الفيدرالية بالقانون الفيدرالي السويسري لحماية البيانات كما يقدم المشورة للأفراد بشأن حماية البيانات، ويجري التحريات ويقدم التوصيات المتعلقة بممارسات حماية البيانات.

ويجب تسجيل بعض ملفات البيانات لدى المفوض الفيدرالي السويسري لحماية البيانات والمعلومات قبل إنشائها. وفي حالة نقل بيانات شخصية خارج سويسرا، لا بد من استيفاء متطلبات خاصة ووفقا للظروف، يجب إخطار المفوض الفيدرالي السويسري لحماية البيانات والمعلومات قبل تنفيذ عملية النقل.

ولقد قامت معظم الأقاليم السويسرية بسن قوانين حماية البيانات الخاصة بها والتي تنظم معالجة أجهزة الأقاليم والأجهزة المحلية للبيانات الشخصية.

ويختلف مفهوم الخصوصية من شخص إلى آخر فقد يكون معناه حماية الخصوصية بترك مساحة للفرد غير قابله للانتهاك عن طريق أي شخص في مسكنه وبهذا المفهوم فأجهزة المراقبة في مكان العمل لا تعد تعديا على الخصوصية.

ووصولا إلى أن مفهوم الخصوصية هو جعل تصرفات بيانات وتحركات الشخص بمنأى عن معرفه واهتمام الغير.

وغالبا ما يختلف ما تعنيه الخصوصية كمفهوم عام عما تعنيه الخصوصية

(1) Donalnd M.U.S. - Swiss Safe Harbor Framework retrived 14 - 3 - 2012 available at http://itlaw.wikia.com/wiki

وفقـا للقانـون. فنوعيـات محـددة فقـط مـن المعلومـات والأنشـطة يقـوم تشريـع الخصوصيـة بحمايتهـا.[1]

ففـي قوانـين حمايـة البيانـات يتـم وصـف معظـم قوانـين الخصوصيـة وبشـكل صحيـح عـلى أنهـا قوانـين حمايـة البيانـات حيـث إنهـا مقصـورة عـلى تنظيـم تـداول الهيئـات للمعلومـات الشـخصية.

---

(1) "African Commission Criticizes Swaziland's Human Rights Record". Freedom House. 25، 2013. P10

الفرع الخامس

خصوصية البيانات في أستراليا

ومثال قوانين الخصوصية التي تحمي الأستراليين - Privacy Laws Protecting Victorians[1]

ففيما عدا قانون حماية المعلومات Information Privacy Act (IPA) هناك ثلاثة قوانين رئيسة أخرى تقوم بحماية خصوصية معلومات الأستراليين.

يحمي قانون السجلات الصحية لسنة 2001 (أستراليا) المعلومات الصحية المتداولة بالقطاعين العام والخاص في أستراليا. ويتم تعريف "المعلومات الصحية" بحيث تشمل المعلومات المتعلقة بالصحة البدنية والعقلية والنفسية للفرد ويمكن أن تتضمن معلومات شخصية يتم جمعها لأجل تقديم الخدمات الصحية للأفراد. ويقوم مفوض الخدمات الصحية Health Services Commissioner بتنظيم قانون السجلات الصحية.[2]

ويغطي قانون الخصوصية لسنة 1988 تداول الهيئات الحكومية الفيدرالية وهيئات الإبلاغ عن الائتمان وأجزاء من القطاع الخاص (باستثناء الشركات الصغيرة) للمعلومات الشخصية (بما في ذلك المعلومات المتعلقة بالصحة). وينظم مفوض الخصوصية الأسترالي Australian Privacy Commissioner قانون الخصوصية. [3]

---

(1) "Aboriginal Protection Act 1869 (Vic)". Documenting Democracy. National Archives of Australia. 2007

(2) "privacy" in Trischa Mann (ed.)، Australian Law Dictionary، Oxford Reference Online، Oxford University Press، accessed (29 August 2011) P.131

(3) Invasion of privacy: Penalties and remedies: Review of the law of privacy: Stage 3" (2009) (Issues paper 14)، New Zealand Law Commission،

ووفقا لقانون ميثاق حقوق الإنسان والمسؤوليات لسنة 2006 الأسترالي، فإن على جميع هيئات الحكومة الأسترالية أن تعمل بالشكل الذي يحمي حقوق الإنسان وهو ما يشمل الحق في الخصوصية.

غالبا ما يعتقد بأن الخصوصية والتكتم مفهوم واحد، وغالبا ما يتم استخدام التعبيرين بشكل متبادل.

إلا أن التكتم يمثل مفهوم قانوني منفصل حيث يتم إعطاء المعلومات لشخص تحت التزام المحافظة عليها كمعلومات مطلوب التكتم عليها (كما على سبيل المثال في سرية التجارة أو المعلومات التي يتم إفضاءها لشخص ما). وعادة ما لا تكون المعلومات المطلوب التكتم عليها متاحة أو معدة لدخول الجمهور عليها في أي وقت ومن الممكن أن تكون معلومات لم يتم تسجيلها بأي شكل من الأشكال المألوفة.

وعلى جانب آخر، يحمي قانون خصوصية المعلومات، المعلومات الشخصية المسجلة أينما احتفظت بها الحكومة الأسترالية أو مقدمي الخدمات المتعاقد معهم.

ولن يؤثر وضع علامة على مستند بأنه: "مطلوب التكتم عليها confiden-tial" أو"معلومات تجارية شديدة الخصوصية commercial - in - confidence" على أي التزامات بالخصوصية قد تنجم نتيجة الاستخدام أو الإفصاح عن المعلومات الشخصية التي يحتويها المستند.

تشمل السرية الأساليب المستخدمة لمنع معرفة الآخرين بالمعلومات. وقد يكون لدى الحكومات والشركات والأفراد أسرار، إلا أن الأفراد فقط هم من لدهم حقوق الخصوصية. فالسرية يمكن أن تساعد شخصا على المحافظة على خصوصيته. وقد تستخدم الحكومات السرية في خدمة المصالح

العامة الأخرى مثل حماية الأمن القومي أو وحدة التحريات المعنية بتنفيذ القانون.

وبالنسبة لحق النشر فهو حق قانوني يحظر على شخص ما من إعادة طبع عمل مشمول بحق النشر دون الحصول على ترخيص من المالك. وعلى الرغم من أنه ينظر أحيانا إلى حقوق النشر على كونها معنية بقانون الخصوصية، فإنها تمثل مفهوما مختلفا.

ويمنح قانون حرية المعلومات لسنة 1982 وبشكل متسع أعضاء حقوق العامة حق الدخول وتصحيح المعلومات في المستندات المتعلقة بشؤونهم الشخصية وأنشطة الحكومة الأسترالية ووكالاتها.

ويمنح القانون حق الدخول على المعلومات فقط للشخص المعني بالمعلومات الشخصية وللمعلومات الشخصية الخاصة به.

ويفيد قانون حماية المعلومات بأن حرية المعلومات تظل الإجراء الذي يجب على الأفراد اتباعه في حالة تلمسهم الدخول على معلوماتهم الشخصية لدى الهيئات الخاضعة لقانون حرية المعلومات. إلا أنه يمكن لقانون حماية المعلومات أن يتيح حق الدخول على المعلومات الموجودة لدى الهيئات غير الخاضعة لقانون حرية المعلومات (IPP 6).

وهو أمر مرتبط بشكل عام بمزودي الخدمة المتعاقد معهم والذين يحتفظون بمعلومات شخصية حيث إن كثيرا من مزودي الخدمة المتعاقد معهم لا يخضعون لقانون حرية المعلومات، وإنما يلتزمون بقانون حماية المعلومات.

ووفقا للعرض السابق نجد أن هناك ثلاثة نماذج تشريعية لتدابير حماية الخصوصية المعلوماتية، وهذه التدابير تعتمد في تطبيقاتها على ما إذا كان منطلق النظام القانوني مجرد الاعتراف بالخصوصية معتمدا على إباحة كل ما يدخل في نطاق الحق، أو باستخدام وسيلة مواجهة الأنشطة التي تمثل اعتداء على الخصوصية، وفي كثير من الدول يستخدم الاتجاهين معا، وبالنسبة للدول

التي توفر حماية فاعلة للخصوصية فإنها قد تستخدم نموذجا أو أكثر لضمان حماية الخصوصية وهذه النماذج هي:

أولاً:القوانين الشاملةCOMPREHENSIVE LAWS:

في العديد من دول العالم ثمة قوانين عامة تحكم عمليات جمع وإدارة ومعالجة البيانات الشخصية في القطاعين العام والخاص، مع وجود جهة لضمان التواؤم مع القوانين وتطبيقها، وهذا هو النموذج الشائع في الدول التي تتبنى قوانين حماية البيانات كما هو حال دول الاتحاد الأوروبي، وهي الدول المتعين عليها التوافق مع دليل حماية البيانات الإرشادي الصادر عن الاتحاد الأوروبي. وقد تم وضع العديد من مثل هذه القوانين في دول خارج الاتحاد الأوروبي أيضا كما هو الحال في كندا وأستراليا. وتسمى أيضا هذه القوانين أو توصف أحيانا بأنها:- CO REGULATORY MODEL.

ثانياً:القوانين القطاعية المخصصةSECTORAL LAWS:

وهي التي تتعلق بقطاع معين، إذ أن بعض الدول، كما هو الحال في الولايات المتحدة الأمريكية، تجنبت سن تشريع عام لحماية الخصوصية، وفضلت إصدار قوانين معينة تحكم قطاعات بعينها، كما هو الحال بسجلات تأجير الفيديو، والخصوصية المالية، وغيرها، وفي مثل هذه الحالة فإن إنفاذ القواعد القانونية يتحقق من خلال آليات مختلفة وليس كما هو الحال بالنسبة للقانون الشامل الذي ينشئ جهة رقابة عامة. ويؤخذ على هذا النموذج أنه يتطلب أن تسن تشريعات جديدة كلما نشأت تقنيات جديدة، ولهذا فإن الحماية تظل متخلفة عن تقنيات الاعتداء، وكمثال على ذلك النقص في حقل حماية البيانات المتعلقة بالجينات مثلا، حيث لا يتم حمايتها بموجب تشريعات الخصوصية حتى الآن، إضافة إلى مشكلة عدم وجود الجهة الحكومية المشرفة. وفي كثير من الدول فإن القوانين القطاعية تستخدم كقوانين مكملة للتشريع العام بما تتضمنه من تفاصيل إضافية في حقل الحماية لطوائف معينة من المعلومات، كالاتصالات وسجلات الشرطة وبيانات الاقتراض للعملاء

وتشريعات الخصوصية المصرفية أو الخصوصية المهنية كما في حقل المحاماة أو غيرها.[1]

وبالنسبة للولايات المتحدة الأمريكية فقد نظمت العديد من القوانين القطاعية المتعلقة بالخصوصية بأيه من قانون حماية البيانات الشخصية المتعلقة بالصحة.

وهناك العديد من القوانين الفيدرالية التي تنظم حماية الخصوصية في قطاعات معينه، ومثال ذلك قانون البنوك الفيدرالي والذي يحتوي على نصوص تنظم استخدام ونشر البيانات الشخصية المتعلقة بالحالة المالية للأفراد وغالبيه القواعد تنظم تقارير الأشخاص الائتمانية وتضع هذه القواعد إطارا عاما يلزم المؤسسات بضمان دقه البيانات والمعلومات الائتمانية وتعطي الأشخاص الحق في الوصول لمثل هذه البيانات، وكذلك هناك قوانين تحكم الاتحادات الائتمانية وتنص صراحة على احترام سريه البيانات المتعلقة بالعملاء.[2]

هناك الكثير من القوانين القطاعية الأمريكية والتي تنص على احترام سرية البيانات الشخصية للأفراد والتي تم الحصول عليها بواسطة المتخصصين في شتى المجالات

ثالثاً:التنظيم الذاتي SELF - REGULATION:

بداية لا بد من الإشارة إلى أن موضوع التنظيم الذاتي للتشريعات هو موقف بشأن موضوعات تقنيات المعلومات عموما، وهو النقيض لما يعرف بالتدخل التشريعي لتنظيم موضوعات تقنية المعلومات، ولكل اتجاه مؤيدوه ومعارضوه، وله إيجابياته وسلبياته، وبالعموم يمكننا القول: إن النموذج

---

(1) الكتاب الثاني من موسوعه القانون وتقنيه المعلومات –الخصوصيه وحمايه البيانات في العصر الرقمي - يونس عرب،2002

(2) Susan W. Brenner، "State Cybercrime Legislation in the United States of America": 7 RICH. J.L. & TECH. 28 (Winter 2001) P.112

الأمريكي للتعامل مع تقنية المعلومات دعا إلى مزيد من تبني فكرة التنظيم الذاتي في حقول التجارة الإلكترونية، ومعايير الخدمات التقنية، وحماية البيانات وأمن المعلومات وغيرها، مع أنه ليس كذلك في حقل الملكية الفكرية مثلا. أما الاتحاد الأوروبي، فإنه يتجه نحو التنظيم الحكومي أكثر، لهذا نجد أن منظماته قد اتجهت دائما إلى توجيه دول الأعضاء إلى إصدار تشريعات تتلاءم مع القواعد المقررة في الأدلة الإرشادية والتوجيهية الصادرة عن منظماته كمجلس أوروبا واللجنة الأوروبية والاتحاد الأوروبي، بل اتجه إلى التنظيم التشريعي الشامل عبر قوانين البرلمان الأوروبي.

وبالتالي فإن بين هذين الرأيين ثمة منطقة رمادية تؤمن بترك كثير من المسائل للتنظيم الذاتي للسوق ووجهات الصناعة والإنتاج، لكنها في الوقت ذاته تتدخل لتنظيم مسائل أخرى، وطبعا كل ذلك وفق الظروف الخاصة بالدولة وتبعا للموضوع محل التنظيم والإستراتيجية الوطنية بشأنه، فإذا كانت أمريكا مثلا تترك مسألة المعايير والمواصفات التقنية للتنظيم الذاتي للسوق فإن هذا الأمر مبرر لما يتوفر من قواعد واسعة في حقل منع التنافس غير المشروع وحقل منع الاحتكار وحماية المستهلك وقواعد منع الغش وإيهام الجمهور، في حين أن دولا نامية أو حتى متقدمة لا يتوفر لها مثل هذا الإطار، لا يكون قرارها بترك تنظيم المعايير للسوق، بل يتعين التدخل من أجل حماية المستهلك وضمان سلامة الخدمات التقنية الموجهة إليه.

وحماية البيانات يمكن أن تتحقق على الأقل نظريا من خلال أشكال عديدة للتنظيم الذاتي التي ومن خلالها تؤسس الشركات الصناعية والتجارية نظاما خاصا للممارسة وللمعايير، يعد سياسة ذاتية لها جميعا، وفي الولايات المتحدة مثلا، فقد فشلت الكثير من جهود التنظيم الذاتي، ربما بسبب تأثر أهداف التنظيم الذاتي بالمصالح الخاصة، إلى جانب مشكلة التواؤم مع هذه السياسات وتنفيذها في مختلف الحقول.

وفي كثير من الدول فإن الكودات الصناعية أنتجت حماية ضعيفة مع

نقص في القوى التنفيذية، وتبرز نماذج عديدة من التنظيم الذاتي في كل من اليابان وأمريكا وسنغافورة.

وبشكل عام، يوجد في مختلف التشريعات الوطنية قواعد تحمي السرية (الأطباء، المحامين، الوظائف العامة، التشريعات العسكرية) أما بالنسبة لقوانين حماية البيانات التي نجمت عن استخدام الكمبيوتر فإنها تتضمن نصوصا جنائية تتعلق بتخزين البيانات بصورة إلكترونية، وقد تطورت في الأعوام الأخيرة لتشمل عمليات الجمع اليدوي للبيانات، وتتكامل هذه التشريعات وتكمل بالقواعد المقررة في قوانين حماية البيانات في القطاعات الخاصة، وبالتالي فإن حماية البيانات الشخصية تجد قواعدها في قوانين حماية البيانات وفي تشريعات حماية البيانات في القطاعات الخاصة، وكذلك في القواعد العامة المقررة لحماية البيانات في القوانين العامة. وكأثر للتطور التاريخي للحماية فإن هناك تباينا واسعا بين النظم الوطنية بشأن الحماية الجنائية لأنشطة جمع المعلومات.[1]

وحديثا أصدرت في جميع دول العالم تشريعات الخصوصية أو قواعد حماية تجميع ومعالجة وتخزين وتبادل البيانات الشخصية.

فمثلا تشريعات جرائم الكمبيوتر، قد تطورت لتشمل جرائم الإنترنت وشبكات الاتصال ضمن مفهوم أشمل (أمن المعلومات) وفي نطاق الاعتراف للمعلومات بالحماية القانونية من كافة الأنشطة التي يكون الكمبيوتر فيها هدفا أو وسيلة أو بيئة للجريمة.

وكذلك مثلا تشريعات الملكية الفكرية في حقل حماية البرمجيات، ومن ثم تطورها لتشمل بقية المصنفات الرقمية، إلى جانب تطورها على نحو يعكس الاتجاهات العالمية في إدراج الملكية الفكرية ضمن تنظيمات التجارة الدولية

---

(1) Bernar،MY،Privacy Rights Clearinghouse، a consumer education and privacy rights advocacy organization 2001. P 89

للتوجه الحاصل نحو الاقتصاد الرقمي والاقتصاد المؤسس على المعرفة ونحو رأس المال الفكريIntelectual Property.[1]

وهناك أيضا تشريعات الأصول الإجرائية الجزائية، وتشريعات الإثبات المتفقة مع عصر الكمبيوتر والمعلومات والتي هي في الحقيقة تطوير لقواعد الإجراءات والإثبات، لكنها أيضا تتصل عضويا بالحقوق الجديدة المعترف بها في ميدان تقنية المعلومات.

بالإضافة إلى تشريعات المحتوى الضار(الحماية من محتوى المعلوماتية على الإنترنت)، ثمة اتجاهات متباينة بين توجه لدمجها مع تشريعات أمن المعلومات كما في أوروبا، أو استقلالها عنها كما في أمريكا - كما سبق الإشارة أن أمريكا تعتمد في قوانين الخصوصية على سياسة القوانين القطاعية.

وأيضا تشريعات معايير الأمن المعلوماتي وتطورها إلى تشريعات المواصفات القياسية لتبادل البيانات والتشفير، وثمة أيضا اتجاهات لاعتبارها جزءا من تشريعات التجارة الإلكترونية في حين هناك اتجاهات لتناول كل موضوع من مواضيعها في تشريع مستقل.

كما توجد أيضا التشريعات المالية والمصرفية فيما يتصل بالمال الإلكتروني وتقنيات الخدمات المصرفية والمالية وفي مقدمتها البطاقات المالية ونظم التحويل الإلكتروني والتي تطورت لتشمل أطرا جديدة في حقل التوجه نحو الأتمتة الكاملة للعمل المصرفي والمالي (البنوك الإلكترونية).

وكذلك تشريعات الاستثمار والتجارة والضرائب والجمارك والاتصالات والأنظمة الحكومية المرتبطة بالمشروعات التقنية أو المتأثرة بتقنية المعلومات.[2]

---

(1) Richard T. De George، ". Intellectual Property Rights،" in The Oxford Handbook of Business Ethics، by George G. Brenkert and Tom L. Beauchamp، vol. 1، 1st ed. (Oxford، England: Oxford University Press، n.d.)، 415-416.

(2) Allen، Julia HThe CERT Guide to System and Network Security Practices. Boston، MA: Addison - Wesley. (2001). P 49

وتشريعات التجارة الإلكترونية (التواقيع الإلكترونية، والتعاقد الإلكتروني، والتسوق الإلكتروني)، وهذه الطائفة تتضمن قواعد تتصل بكافة حقول تقنية المعلومات لأنها أثارت تحديات فيها جميعا، لهذا ثمة حقيقة أن التجارة الإلكترونية وحدها برغم أنها آخر حلقات تقنية المعلومات في الوقت الراهن فإنها الإطار الأوسع المؤهل لتوحيد قواعد قانون الكمبيوتر.

وعلى الصعيد الدولي فهناك تشريعات (اتفاقيات ومعاهدات) الاختصاص والقانون المطبق على المنازعات القضائية في بيئة الإنترنت (بشكل خاص منازعات الملكية الفكرية ومنازعات التجارة والأعمال والبنوك الإلكترونية).

ومما سبق نخلص إلى أن هناك عده أنظمة تشريعية لتنظيم الخصوصية المعلوماتية وأهم هذه الأنماط تقسيم القوانين التي تحكم خصوصية البيانات من حيث جهة التنظيم وقد ثبت أن القوانين القطاعية والتي تمنح لكل قطاع وضع نظام قانوني لحماية البيانات الشخصية وفقا لمتطلبات القطاع وتطوراته هو أفضل الأنظمة حيث يمكن ذلك النظام من فرض الحماية القصوى للبيانات إذ أن كل جهة على دراية تامة بالتفاصيل التقنية التي يمكن أن تكون مدخلا للتعدي على خصوصية البيانات وكذلك وضع حد عادل للاستخدام والنقل والإفصاح عن البيانات بالقدر الذي لا يعيق عمل تلك الجهات، ويعتبر النظام القانوني الأمريكي نظام يحتذى به في هذا المجال.

علما بأن الدول العربية لم تصل بعد لتشريعات واضحة تضمن حماية خصوصية البيانات الرقمية والمتداولة عبر الإنترنت، فيما عدا القليل من المحاولات التشريعية في حقل الملكية الفكرية.

المطلب الثالث

الإطار العام للقوانين التي تحمي الخصوصية في الدول العربية

لما أثيرت فكرة خصوصية البيانات تعين البحث في:

- إطار حماية البيانات وتشريعات تقنية المعلومات في البيئة العربية **(الفرع الأول)**.
- مع توضيح موقف المشرع العربي في نطاق الملكية الفكرية والمصنفات الرقمية **(الفرع الثاني)**.
- وكذلك النطاق القانوني لحماية برامج الكمبيوتر وقواعد البيانات في البيئة العربية**(الفرع الثالث)**.
- وتثور إشكالية حماية البرمجيات وقواعد البيانات **(الفرع الرابع)**.
- وموقف المشرع المصري من الخصوصية الرقمية **(الفرع الخامس)**.

الفرع الأول

إطار حماية البيانات وتشريعات تقنية المعلومات في الوطن العربي

أولاً: في مصر

نجد أن مكافحة جرائم الكمبيوتر في مصر تمت معالجتها بقوانين عامة كالقانونين المدني والجنائي. فنجد في المادة التاسعة من القانون 260 لسنة 1980 في شأن الأحوال المدنية المعدل بالقانونين رقمي 11 لسنة 1965 و158 لسنة 1980 على أن البيانات التي تحويها سجلات الأحوال المدنية تعتبر سرية، وقد جاء بالمذكرة الإيضاحية للقانون: "أنه لما كانت هذه السجلات تحوي أدق البيانات عن حالة الشخص فقد أسبغت عليها السرية حتى يطمئن كل شخص على ما يقدمه من بيانات. إن نطاق السرية يمتد إلى كل من لا يفرض عليه واجبه طبقا لقانون الأحوال ولائحته التنفيذية والقرارات المنفذة له الاطلاع على هذه البيانات، وذلك ما لم تصدر سلطة قضائية أو سلطة تحقيق قرارا بالاطلاع عليها أو فحصها لأن الصالح العام يفضل صالح الشخص في المحافظة على سرية بياناته، وباعتبار هذه البيانات سرا فإن إفشائها من قبل الموظف الملزم بكتمانها يوقعه تحت العقاب المنصوص عليه في المادة 310 من قانون العقوبات".[1]

ثانياً: في اليمن

وفي اليمن نجد أن القانون الجنائي قد نص على مجموعة من المقتضيات ترمي إلى مكافحة الجريمة في مجال الاعتداء على الأموال كـ: السرقة والاحتيال والابتزاز وخيانة الأمانة والتزوير وذلك في المواد التالية:(210،310،313،318) من القانون رقم (12) لعام 1994 م بشأن

(1) أشرف فهمي خوخة، التشريعات الإعلامية بين الرقابة وحرية التعبير، مكتبة الوفاء القانونية، الإسكندرية،2013.

الجرائـم والعقوبـات، وكـذا في مجـال الاعتـداء عـلى الأشـخاص كجريمـة التهديـد، انتهـاك حريـة المراسـلات، الاعتـداء عـلى حرمة الحيـاة الخاصـة، والتهديد بإذاعـة الأسرار الخاصة كـما هـي ثابتة المـواد257.256.255.254 مـن القانون نفسـه.[1]

إلا أنـه ومـع الاسـتخدام المتزايـد لتقنيـة المعلومـات في شـتى مجـالات الحيـاة، وظهـور المعلوماتيـة وتطبيقاتهـا المتعـددة ومـا ترتـب عـلى ذلـك مـن ظهـور تقنيـات جديـدة في ارتـكاب الجريمـة التقليديـة كالاسـتيلاء عـلى الأمـوال عـن طريـق الاحتيـال المعلومـاتي أو كإرسـال بريـد يتضمـن تهديـد بالقتـل أو اخـتراق شـبكات المعلومات، جعل القانـون الجنـائي أمـام قصـور بـين في مواجهـة تلـك الجرائـم.

وهـذا يرجـع في الأسـاس إلى أن مـواد القانـون الجنـائي اليمنـي نصـوص تقليديـة وضعـت أساسـا لحمايـة الأشـياء الماديـة في مواجهـة صـور الاعتـداء التقليـدي عليهـا، وبالتـالي فقـد تعـذر تطبيـق تلـك النصـوص عـلى حـالات الاعتـداء عـلى المكونـات غـير ماديـة للأنظمـة المعلوماتيـة.

ثالثـا: في المملكة العربية السـعودية:

فقـد وافـق مجلـس الـوزراء في المملكـة العربيـة السـعودية سـنة 2007عـلى نظامـي مكافحـة جرائـم المعلوماتيـة والتعامـلات الإلكترونيـة، وكان ذلـك للحـد مـن وقـوع الجرائـم المعلوماتيـة وتحديـد الجرائـم المسـتهدفة بالنظـام والعقوبـات المقـدرة لـكل جريمـة أو مخالفـة، وتحديـد جهـة الاختصـاص بمتابعتهـا وتطبيـق العقوبـات.[2]

ويرمـــي هـــذا القانـــون إلى تأمـــين اســـتخدام أجهـــزة الكمبيوتـــر وشـــبكة

(1) العادلي محمود صالح،الجرائم المعلوماتية - ماهيتها وصورها، ورقة عمل مقدمة لورشة العمل الإقليمية حول تطوير التشريعات في مجال مكافحة الجرائم المعلوماتية، مسقط للفترة 4 - 3 إبريل، 2006. ص23

(2) *محروس نصار غايب، الجريمة المعلوماتية،2010 ص18 بحث منشور على الرابط http://www.iasj.net/iasj?funcfulltext&aId28397

المعلومات الدولية (الإنترنت) من عبث العابثين الذي يتمثل في ارتكاب جرائم الأموال وجرائم الآداب وجرائم الإرهاب وجرائم السب والقذف، وجرائم غسل الأموال.

رابعاً: في الإمارات العربية:

وفي الإمارات العربية المتحدة صدر القانون الاتحادي رقم 2 لسنة 2006 في شأن مكافحة جرائم تقنية المعلومات، حيث تنص المادة 2 من القانون على أن: "كل فعل عمدي يتوصّل فيه بغير وجه حق، إلى موقع أو نظام معلوماتي، سواء بدخول الموقع أو النظام، أو بتجاوز مدخل مصّرح به، يعاقب عليه بالحبس وبالغرامة، أو بإحدى هاتين العقوبتين، فإذا ترتّب على الفعل إلغاء أو حذف أو تدمير أو إفشاء أو إتلاف أو تغيير أو إعادة نشر بيانات أو معلومات، فيعاقب بالحبس مدة لا تقلّ عن 6 أشهر، وبالغرامة أو بإحدى هاتين العقوبتين".

فيما تنص المادة 3 من القانون السالف الذكر على أن كل: " من ارتكب أياً من الجرائم المنصوص عليها في البند 2 من المادة 2 من هذا القانون، أثناء أو بسبب تأدية عمله، أو سهّل ذلك للغير، يعاقب بالحبس مدة لا تقل عن سنة، ويغرّم ما لا يقلّ عن 20 ألف درهم، أو بإحدى هاتين العقوبتين".[1]

خامساً: في عمان:

بموجب المرسوم السلطاني رقم 2001/72 المنشور في الجريدة الرسمية العمانية رقم 698 تاريخ 2001/7/1 تم تعديل بعض أحكام قانون الجزاء العماني رقم 7 لعام 1974، ومن ضمن هذه التعديلات: إضافة الفصل الثاني مكرر على الباب السابع تحت عنوان جرائم الحاسب الآلي (المواد 276 مكررا و276 مكرر 1 و276 مكرر 2 و276 مكرر 3 و276 مكرر 4.

---

(1) عبد الصبور عبد القوي علي، الجريمة الإلكترونية والجهود الدولية للحد منها، كلية الحقوق - جامعة بني سويف 2012 ص 10.

وقد نصت المادة (276 مكرراً):على أنه يعاقب بالسجن مدة لا تقل عن ثلاثة أشهر ولا تزيد عن سنتين وبغرامة من مائة ريال إلى خمسمائة ريال أو بإحدى هاتين العقوبتين كل من تعمد استخدام الحاسب الآلي في ارتكاب أحد الأفعال الآتية:

1 - الالتقاط غير المشروع للمعلومات أو البيانات.

2 - الدخول غير المشروع على أنظمة الحاسب الآلي.

3 - التجسس والتصنت على البيانات والمعلومات.

4 - انتهاك خصوصيات الغير، أو التعدي على حقهم في الاحتفاظ بأسرارهم.

5 - تزوير بيانات أو وثائق مبرمجة أياً كان شكلها

6 - إتلاف وتغيير ومحو البيانات والمعلومات.

7 - جمع المعلومات والبيانات وإعادة استخدامها.

8 - تسريب المعلومات والبيانات.

9 - التعدي على برامج الحاسب الآلي سواء بالتعديل أو الاصطناع.

10 - نشر واستخدام برامج الحاسب الآلي بما يشكل انتهاكاً لقوانين حقوق الملكية والأسرار التجارية.

كما نصت المادة (276 مكرراً)(1): على أنه: " يعاقب بالسجن مدة لا تقل عن ستة أشهر ولا تزيد عن سنتين وبغرامة لا تقل عن مائة ريال ولا تزيد على خمسمائة ريال أو بإحدى هاتين العقوبتين كل من استولى أو حصل على نحو غير مشروع على بيانات تخص الغير تكون منقولة أو مختزنة أو معالجة بواسطة أنظمة المعالجة المبرمجة للبيانات.

ونصت المادة (276) مكرراً (2): على أنه: " تضاعف العقوبة إذا

ارتكبت الأفعال المشار إليها في المادة (276) مكرراً و(276) مكرراً (1) من مستخدمي الكمبيوتر.

ونصت المادة (276) مكرراً (3):على أنه" يعاقب بالسجن مدة لا تزيد على خمس سنوات وبغرامة لا تجاوز ألف ريال كلا من:

1 - قام بتقليد أو تزوير بطاقة من بطاقات الوفاء أو السحب.

2 - استعمل أو حاول استعمال البطاقة المقلدة أو المزورة مع العلم بذلك.

3 - قبل الدفع ببطاقة الوفاء المقلدة أو المزورة مع العلم بذلك.

ونص في المادة (276) مكرراً (4): على أنه:" يعاقب بالسجن مدة لا تزيد على 3 سنوات وبغرامة لا تجاوز خمسمائة ريال كلا من:

1 - استخدم البطاقة كوسيلة للوفاء مع علمه بعدم وجود رصيد له.

2 - استعمل البطاقة بعد انتهاء صلاحيتها أو إلغائها وهو عالم بذلك.

3 - استعمل بطاقة الغير بدون علمه.

وبإمعان النظر في هذه النصوص نجد المشرع العماني اختار طريق إضافة النصوص الخاصة إلى القسم الخاص في قانون العقوبات (التشريع الجزائي العام)، ولم يختر طريقة سن تشريع خاص، كما لم يختر نموذج النص على مساواة الأموال المنقولة المادية بغير المادية لأغراض انطباق النصوص المتعلقة بالجرائم الواقعة على الأموال وحسنا فعل في هذا الشق إذ تتمايز كما عرفنا صور جرائم الكمبيوتر من حيث مبناها وطبيعتها وسلوكياتها عن الجرائم التقليدية، ليس فقط من ناحية محل الجريمة.

وجرم المشرع العماني 10 صورا جرمية في المادة 276 مكررا، امتدت لتجريم صور جرمية من تلك التي تتعلق بحماية الخصوصية وصور جرمية تتصل بحماية حق المؤلف والأسرار التجارية، وصور جرمية تتعلق بالالتقاط

والدخول غير المصرح به والإتلاف والاستيلاء والإفشاء والتجسس أو ما يعرف بطائفة الجرائم الواقعة على المعطيات ذات القيمة الاقتصادية، وهذا النص يثير التساؤل بشأن مدى توافقه أو تعارضه مع النصوص الخاصة بالحماية الجزائية في قوانين الملكية الفكرية التي خضعت جميعا لإعادة البناء في السلطنة وسن تشريعات جديدة بشأنها تضمن بعضها نصوصا جزائية، بمعنى أن بعض الصور تتصل بتنظيم قانوني آخر قائم في الدولة وهو ما قد يخلق تعارضا أو يثير تحديات في التطبيق العملي.

كما أنه بالصورة التي تضمنها نص على بعض صور جرائم الخصوصية أو انتهاك حرية الشخص في بياناته الخاصة المعالجة آليا، فلم ينص على بقية صور الاعتداء على الخصوصية كنقل البيانات دون أذن أو استغلالها في نشاط غير المعدة له. ثم أغلق النص الطريق على وضع تشريع تكاملي في ميدان الخصوصية يتناول الجوانب المتعلقة بحماية الأفراد من مخاطر الجمع الحكومي للبيانات ومسائل تعيين جهات الرقابة على عمليات جمع ومعالجة ونقل البيانات وغيرها الكثير من المسائل الموضوعية والإجرائية ذات الصلة بموضوع الخصوصية إضافة إلى بقية صور الحماية الجزائية خاصة من الموظفين المناط بهم جمع وتداول واستخدام البيانات الشخصية.

المادة 276 مكررا 1 نصت على تجريم صورة إضافية وهي الاستيلاء على البيانات لكنها لم تنص على سرقة وقت الكمبيوتر أو صور أخرى متصلة بتعطيل عمل الأنظمة الإلكترونية، كما لم تتضمن النصوص ولم تتعرض لاحتيال الكمبيوتر وان كانت النصوص تضمنت بعض صوره من الناحية الفنية.

أما المادة 276 مكررا 4 فعالجت ثلاث صور من صور إساءة استخدام بطاقات الوفاء الإلكترونية، ويؤخذ على النص تقيده باصطلاحات مقيدة في حين كان يمكنه أن يكون أكثر اتساعا حين يجرم صور الاعتداء المذكورة على كل أنواع البطاقات منعا للدفع بأن البطاقة محل الاعتداء ليست بطاقة وفاء.

هـذه الحقائـق التـي بـدت واضحـة أمـام جهـات التشريـع والقضـاء في النظـم المقارنـة بعـد جـدل طويـل وتقييـم واسـع، اسـتدعت أن تتدخـل العديـد مـن الـدول الأجنبيـة - التـي تقـارب قوانينهـا قوانيننـا العقابيـة العربيـة بـل تعـد أكـثر اتسـاعا منهـا في هـذا الجانـب - أقـول اسـتدعى تدخـل المشرعـين في هـذه الـدول لتعديـل القوانـين الجنائيـة أو سـن قوانـين جديـدة لمواجهـة هـذه الظاهـرة المسـتجدة، فبعـض الـدول عدلـت قوانينهـا بالنـص صراحـة عـلى إنـزال معطيـات الكمبيوتـر منزلـة المـال المـادي المنقـول وذلـك لتحقـق إمكانيـة تجريـم المعتديـن على هذا المـال بنصـوص جرائم السرقة والاحتيـال والإتـلاف وغيرهـا، وبعضهـا اتجـه نحو سـن تشريعـات مسـتقلة لتجريم جرائم الكمبيوتـر أو اسـتحداث نصـوص مسـتقلة وإضافتهـا إلى تشريعاتهـا القائمـة، وهـذا المسـلك امتـد ليشـمل الـدول نفسـها التـي نحـت المسـلك الأول فعـادت لسـن تشريعات جديـدة لعـدم كفايـة التعديـلات التـي أحدثتهـا.

ونخلـص مـما سـبق أن نصـوص التجريـم المقـررة في قوانـين العقوبـات العربيـة (عـدا قانـون واحـد هـو قانـون الجـزاء العـماني الـذي لحقـه التعديـل بموجـب القانـون 72 لعـام 2001 وأدخـل أربعـة نصـوص تجـرم عـددا من صـور جرائـم الكمبيوتـر) عاجزة عـن مواجهـة خطـر جرائـم الكمبيوتـر، ونقصـد هنا خطـر الجرائـم الواقعة عـلى البيانات الماليـة أو المتعلقـة بالذمـة الماليـة، فـإذا مـا أضيـف إلى هـذا الواقـع عدم وجـود نصوص تجـرم أفعـال الاعتـداء عـلى البيانـات الشـخصية المخزنـة في نظـم المعلومـات وبنوكهـا أو نصوصـا تحمـي البيانـات مـن خطـر المعالجـة الآليـة وتكفـل حمايـة الخصوصيـة – بوجه عـام طبعـا وفي جميـع الـدول العربيـة– فإننـا نكـون أمـام واقـع قاتـم لـن تزيـل قتامتـه غـير جهـود وتدابـير تشريعيـة حثيثـة لسـد النقـص الحاصـل وإيجـاد قواعـد تحيـط بهـذا النمـط الخطـر والمسـتجد مـن أنمـاط الإجرام.

وبالتـالي نسـتنتج الحقائق التالية:

الحقيقـة الأولى: وهـي أن جرائـم الكمبيوتـر تسـتهدف المعطيـات ذات الطبيعـة المعنويـة:

فعندمـا يكـون الكمبيوتـر هدفـا للجريمـة فـإن السـلوك يسـتهدف المعلومـات المخزنـة فيـه أو المنقولـة منـه أو إليـه وعندمـا يكـون وسـيلة لارتـكاب الفعـل، فـإن السـلوك يسـتهدف بيانـات تمثـل قيـما ماليـة أو اعتبـارا ماليـا، ويجـري الفعل أو السـلوك بتوسـل طـرق تقنيـة في بيئـة معنويـة وليسـت في بيئـة سـلوكيات ماديـة.

وعندمـا يكـون بيئـة للجريمـة فـإن محتـوى الفعـل غـير المـشروع هـو المعلومـات غـير المشروعـة كـما هـو الحـال في جرائـم المحتـوى المعلومـاتي الضـار.

الحقيقـة الثانيـة: إن مبـدأ الشرعيـة الجنائيـة يمنـع المسـاءلة الجنائيـة مـا لم يتوفر النـص القانوني:

فـلا جريمـة ولا عقوبـة إلا بنـص، ومتـى مـا انتفـى النـص عـلى تجريـم مثـل هـذه الأفعـال التـي لا تطالهـا النصـوص القائمـة امتنعـت المسـؤولية وتحقـق القصـور في مكافحـة هكـذا جرائـم.

الحقيقـة الثالثـة: إن القيـاس في النصـوص الجنائيـة الموضوعيـة محظـور وغـير جائز، ويـكاد ينحـصر في الحقـل الجنـائي بنصـوص الإجـراءات الجنائيـة كلـما كانت أصلـح للمتهم:

ومـؤدى ذلـك امتنـاع قيـاس أنمـاط جرائـم الكمبيوتـر عـلى الجرائـم التقليديـة التـي تسـتهدف الأمـوال والاعتبـار المـالي. ومن جهـة أخـرى لا يصلح القيـاس على نصوص خاصـة بنـوع مـن الجرائـم كقيـاس سرقـة المعلومـات أو سرقـة وقـت الكمبيوتـر عـلى الاسـتيلاء عـلى القـوى المحـرزة كالكهربـاء لتخلف علـة القياس ولأن هـذه نصوص شرعت خصيصـا لتطـال الأنمـاط التـي تنظمهـا وهـي نصـوص خاصـة لا يتوسـع في القيـاس عليهـا بـل لا نبالـغ إذا قلنـا إن جـزءا مـن النصـوص الخاصـة يعـد اسـتثناء عـلى أصل والاسـتثناء لا يتوسـع فيـه.

وهناك عدو نتائج تستنبط من الواقع العربي في حماية المعلومات وتشريعات تقنية المعلومات بوجه عام (عدا تشريعات حماية المصنفات الرقمية في نطاق الملكية الفكرية):

أولا: برغم وجود أطر قانونية تنظم بنوك المعلومات وقواعد البيانات المركزية في عدد من الدول العربية إلا أنه لا يوجد تشريع متكامل في حقل الخصوصية في أي من الدول العربية، وثمة أفكار أو مشاريع في هذا الحقل في الأردن والإمارات، وبالتالي تظل البيانات المتعلقة بالأشخاص والحياة الخاصة دونما تنظيم كاف ودونما حماية كافية رغم الحاجة الملحة إلى ضبط استخدام ومعالجة ونقل البيانات الشخصية في البيئة الرقمية، وما تتيحه أنشطة الاعتداء على هذه البيانات من مساس جوهري بحقوق الإنسان بل وبثقة المستهلك بوسائل التقنية واستخداماتها.[1]

ثانياً - باستثناء التعديل الذي حصل على قانون البيانات الأردني ومشروع تعديل قانون أصول المحاكمات اللبناني، لم تشهد قوانين الإثبات العربية تعديلات في حقل حجية مستخرجات الكمبيوتر والمواد الإلكترونية في النزاعات الحقوقية والتجارية [2].

ثالثاً: في ميدان التجارة الإلكترونية والأعمال الإلكترونية، أقرت الأردن ودبي وتونس تشريعات عالجت موضوع التجارة الإلكترونية، وتكاد تتفق جميعا في بنائها الذي يعتمد على القانون النموذجي للتجارة الإلكترونية الذي وضعته لجنة اليونسترال (لجنة قانون التجارة في الأمم المتحدة) عام 1996.[3]

---

(1) يونس عرب. الخصوصية وحماية البيانات في البيئة العربية. دائرة المكتبة الوطنية، 2002 ص 2.

(2) ويمكن القول إن الاتجاه التشريعي منذ عام 1997 في الأردن يتجه إلى الاعتراف بقيمة القيود الإلكترونية في مختلف قطاعات النشاط كما هو الحال في الاعتراف بها لإثبات ملكية الأسهم في أسواق التداول المالي والاعتراف بها لإثبات التصرفات والمراكز القانونية بالنسبة لتسجيل مصنفات الملكية الصناعية لدى دوائر وزارة الصناعة والتجارة وغيرها.

(3) رأفت رضوان، عالم التجارة الإلكترونية، المنظمة العربية للتنمية الإدارية، القاهرة =

ومع ذلك، وحتى في هذه الدول التي وضعت هذه التشريعات، فإن النقص التشريعي لا يزال قائما في الحقول التي تتيح تفعيل هذه التشريعات ووضعها موضع التطبيق، فليس ثمة تنظيم لسلطات توثيق المعاملات الإلكترونية وليس ثمة تشريعات للمعايير الأمنية أو المعايير القياسية لخدمات التقنية وليس ثمة حسم لكثير من المشكلات الرئيسة في ميدان التجارة الإلكترونية كمسائل الضرائب على الإنترنت ومسائل الخصوصية وغيرها، ولا أبالغ إن قلت إن سياسات الاستنساخ التشريعية والنقل والترجمة عن القوالب الجاهزة دون مراعاة للنظام القانوني أو تعمق في المسالة محل التنظيم أدى إلى ولادة تشريعات تشوبها النواقص وتطال أحكامها المطاعن، والأهم من ذلك أنها لم تتح تحقيق الغرض الذي وضعت من أجله.

رابعاً: لم يجر إقرار أي تشريع عربي في حقول المعايير الأمنية أو القياسية لتقنية المعلومات أو في حقول الإجراءات الجنائية الملائمة للأفعال التي تستهدف المعلومات وقواعدها وشبكاتها. [1]

خامساً: انحصر التلاقي بين النظام القانوني العربي وبين موجات تشريعات تقنية المعلومات في ميدان حماية المصنفات الرقمية وتحديدا حماية البرامج وقواعد البيانات والدوائر المتكاملة عبر تشريعات حق المؤلف أو تشريعات خاصة كما في قوانين حماية طبوغرافيا الدوائر المتكاملة، وليس ثمة أي تشريع في الوقت الحاضر ينظم حماية عناصر الإنترنت ومواقع المعلوماتية.[2]

ويرى الباحث أنه في ضوء قراءة التجربة العربية - حتى الآن - في

=1999، ص18.

(1) المحامي يونس عرب، التدابير التشريعية العربية لحماية المعلومات والمصنفات الرقمية، ورقة عمل مقدمة أمام الندوة العلمية الخامسة حول دور التوثيق والمعلومات في بناء المجتمع العربي النادي العربي، للمعلومات - دمشق

(2) الكتاب الثاني دليل امن المعلومات والخصوصية، ج1، جرائم الكمبيوتر والإنترنت ط1، منشورات اتحاد المصارف العربية، بيروت 2002 ص236

التعامل مع العصر الرقمي واحتياجاته التشريعية، أننا نلحظ تخبطا في التعامل مع المتطلبات التشريعية لتقنية المعلومات، وهو أشبه بحالة التخبط التي شهدتها النظم المقارنة في مطلع السبعينات وخلال الثمانينات، ولا تزال تشهد بعضا من ملامحه في عدد من مسائل تقنية المعلومات في الوقت الحاضر، وفي هذا السياق، يلمس المتابع عدم وضوح الرؤية، ويلمس اتجاه المؤسسات التشريعية في الدول النامية – ومنها العربية - إلى حلول مبتسرة وليست حلولا كافية تدرك التحديات التقنية ذاتها وتدرك حالة التغير والتطور في الاحتياجات القانونية لمواجهة العصر الرقمي، وتدرك أكثر أن الحلول المقتبسة دون إعادة تواؤم واع ومدروس على الأقل، حلول معطلة وليست فاعلة لاعتبارات اجتماعية وسياسية واقتصادية وقانونية، حتى أننا لا نكون مبالغين إن قلنا إن هذه الحلول الجزئية المقتبسة تزيد التحديات ولا توفر حلولا لها، كما أنها في بعض الأحيان تقيم مزيدا من العوائق نحو الأهداف النبيلة في خطط توظيف التقنية بدلا من أن تذلل هذه العوائق.

إن شيوع الكمبيوتر وفيما بعد الاتجاه نحو التشبيك عبر مختلف أنواع شبكات المعلومات وفي مقدمتها الإنترنت وبناء شبكات وقواعد المعلومات، أفرز حاجة ملحة للتدخل من أجل حماية أمن المعلومات وحماية الخصوصية والتنظيم الصحيح لحماية الملكية الفكرية ومراعاة آثارها على المجتمع، ومن أجل حماية المستهلك والاعتراف بالحجية وملاءمة الوسائل الإلكترونية للتصرفات القانونية بالقدر نفسه من الملاءمة المقبولة والمعترف بها للوسائل غير الإلكترونية، إلى جانب أهمية تنظيم معايير ومقاييس التقنية وحماية المستخدم في نطاقها وتنظيم البنى التحتية ضمن تدابير تكفل نماء وتوظيف التقنية بشكل صحيح وملائم لحاجات المجتمع.

إن أخطر ما يواجه فعالية نظم حماية المعلومات وفعالية الأدوات التشريعية لتنظيم استخداماتها وتطبيقاتها وصورة المعالجات الجزئية للتحديات القانونية المتصلة بتقنية المعلومات، تلك المعالجات التي يظن البعض أنها الحل القانوني الكامل، في حين أنها قطعة فسيفسائية من لوحة

قانون تقنية المعلومات، والأخطر أنها حلول لم تدرك عاملين رئيسين، الأول، أننا نتحدث عن تنظيم مسائل أثيرت منذ منتصف الستينات تقريبا، ودراسة مسيرتها التاريخية يدلنا على اتجاهات تطورها مستقبلا، فإن لم يدرك الماضي ولم يستشرف المستقبل أصبحنا كأننا ننظم الحاضر فقط، فإن أضفنا أنه حاضر غيرنا لا حاضرنا أصبحت المخاطر أكثر عمقا وأكثر احتمالية للتحقق وأصبح التدبير غير ذي أثر. والثاني، أنها مسائل تعرضت للتشوه أو على الأقل غياب المقاييس العلمية لتبيان الصواب والخطأ بشأنها، وكبديل على إعادة التقييم الواعي من قبل الجهات المتخصصة في هذا الحقل، اعتمدنا فكرة الثقة بتقدير جهات خارجية أقل ما توصف أنها في حد ذاتها لا تزال تعاني تحديات الصواب والخطأ وتجرب وتعيد التجربة، مما يعني أن ما نثق به محل شك، ولهذا يصبح التدبير ذاته محل شك.

وفي هذا السياق لن يكون كافيا القول في نظام قانوني ما إن قانون التواقيع الرقمية مثلا قد حل مشكلة التجارة الإلكترونية أو حل مشكلات وتحديات الحكومة الإلكترونية أو الأعمال المصرفية الإلكترونية، أو أنه فعلا سيحل مشكلة الأعمال اللاسلكية الخلوية الآخذة في النماء على نحو أفرز مفهوما جديدا لتبادل المعطيات وأداء الخدمات عن بعد، فتنظيم حجية المعاملات الإلكترونية مثلا مجرد جزئية في فضاء تملؤه التحديات، تلك التحديات التي تمتد إلى مسائل التنظيم القانوني لأمن المعلومات التي تنتمي بدورها إلى تجربة تاريخية وتشريعية لها مزاياها ومتطلباتها، وتمتد لمسائل الخصوصية التي أصبحت تنظم ضمن أدوات تتعدد طبيعتها تمتاز بالشمولية وكثرة المسائل محل التنظيم التي تفوق تدبيرا تشريعيا جزئيا، وكذلك مسائل الملكية الفكرية للعناصر الرقمية ومسائل التقاضي وإجراءاته في هذه البيئة وغيرها الكثير من التحديات.

وبالتالي فنشير إلى الحاجة الملحة إلى حزمة متكاملة من التشريعات في حقل تقنية المعلومات، تمتد لتغطية عناصر أساسية أربع:

الأول: الاعتراف القانوني بالمعلومات ووسائل حمايتها المدنية والجزائية في النظام القانوني، وهذا الأساس يغطي طائفة تشريعات الأمن والخصوصية والسرية وبناء قواعد البيانات ومواقع المعلوماتية إضافة إلى القواعد الإجرائية وقواعد الإثبات المتصلة بهذه الموضوعات وما يتعلق بمنازعاتها ودعاويها.

والثاني: التنظيم الملائم لوسائل التقنية ومعاييرها ومواصفاتها وتغطي مساحة المسائل المتصلة بتوظيف التقنية والاستثمار والاتجار بها وتوريد الخدمات وإدامتها، إنتاجا ونقلا وتبادلا، وقواعد المنافسة المشروعة في القطاع وغيرها.

والثالث: الاعتراف القانوني بصلاحية الوسائل الإلكترونية في بيئة الأعمال والخدمات والاستثمار، وهذه تتصل بالإطار القانوني للتجارة الإلكترونية والحكومة الإلكترونية والبنوك الإلكترونية والأعمال اللاسلكية.

والرابع: الاعتراف القانوني بمصالح المستهلك والمستخدم وتوفير الحماية القانونية من عيوب ومخاطر التقنية وتطبيقاتها.

هذه الأسس الأربعة تفرز عشرات التشريعات وليس تشريعا واحدا فقط أو تفرز تشريعا شموليا قادر على تغطيتها، لأن التنظيم القانوني لتقنية المعلومات يمتد لتغطية مختلف فروع القانون المدني والجزائي والتجاري والإداري والمالي والمصرفي وتشريعات الإجراءات والإثبات، والتشريعات المرتبطة بمختلف الخدمات وفي مقدمتها الاتصالات، وتلك الخاصة بتنظيم الإنتاج الصناعي بمختلف مسائله وتشريعات الثقافة والإعلام والمعايير والمقاييس وحقوق الإنسان وغيرها. والأهم يراعي التواؤم بينها كي لا نخلق في النظام القانوني الواحد ما يهدم أحكامه وما يوفر ثغرات النفاذ التي تستغل التناقض في المعالجة والتباين في الحلول التشريعية.

الفرع الثاني

النظام القانوني العربي للملكية الفكرية وحماية المصنفات الرقمية

أولاً: في نظام الملكية الفكرية العربي بوجه عام:

اهتمت الدول العربية مبكرا بمسائل الملكية الفكرية، حتى إننا نجد بعضها قد ساهم في الجهد الدولي لحماية الملكية الفكرية اعتبارا من القرن التاسع عشر كما هو حال الجمهورية التونسية، وأن عددا من الدول العربية كان من الدول الأساسية في عضويتها لعدد من اتفاقيات الملكية الفكرية الدولية كما سنوضح تاليا.

إن استجابة الدول العربية لحماية الملكية الفكرية تبدو عالية بالنظر لموجات التشريعات التي تظهر فيها، فإذا كانت الخمسينات قد شهدت موجة تشريع واسعة في غالبية الدول العربية في حقل حماية براءات الاختراع والعلامات التجارية والتصاميم الصناعية، فإن الثمانينات والتسعينات شهدت موجة واسعة من التدابير التشريعية في حقل حماية حق المؤلف والحقوق المجاورة وشهد مطلع التسعينات إقرار قوانين عديدة أو تعديل القوانين القائمة لجهة حماية برامج الحاسوب وقواعد البيانات ضمن قوانين حماية حق المؤلف.[1]

ومن الملاحظ أن الاتفاقية تلزم الدول الأعضاء باتباع سياسات عامة يتعين أن تتفق مع الاتجاه العام ولكن قد تختلف في التفاصيل من دولة إلى أخرى.[2]

---

(1) عمر عدنان العوبثاني في تقريره " العرب والتجارة الإلكترونية ومخاوف الدوت كوم " منشور بالملحق الاقتصادي لجريدة الخليج الإماراتية، العدد8116 في2001.

(2) د.أبو العلا النمر، الحماية الوطنية للملكية الفكرية في ظل اتفاقية الجوانب المتصلة بالتجارة من حقوق الملكية الفكرية. دار أبو المجد للطباعة، الطبعة الثانية،1998 وص 33.

أما نهاية التسعينات وعام 2000 فقد شهدت موجة تشريعية في ميدان حماية الأسرار التجارية والمؤشرات الجغرافية وطبوغرافيا الدوائر المتكاملة وحماية أصناف النباتات الدقيقة، مترافقا مع التطوير والتعديل على قوانين الملكية الفكرية الأخرى، ومرد ذلك تلبية متطلبات العضوية في منظمة التجارة العالمية وما يوجبه ذلك من تلبية متطلبات اتفاقية تربس (اتفاقية الملكية الفكرية) التي نصت على هذه الحماية.

وتمثل الأردن وسلطنة عمان وتونس النماذج الأكثر استجابة من بين الدول العربية لهذه المتطلبات حيث تكاد تتطابق التدابير التشريعية فيها والتي تعكس تقيدا بما تتطلبه اتفاقية تربس في الموضوعات المشار إليها.

أما بالنسبة لموقف الدول العربية من الاتفاقيات الدولية في حقل الملكية الفكرية، فيمكننا القول إن غالبية الدول العربية هي أعضاء في أهم ثلاث اتفاقيات وهي اتفاقية إنشاء المنظمة العالمية للملكية الفكرية، واتفاقية برن للملكية الأدبية واتفاقية باريس للملكية الصناعية، أما الاتفاقيات الأخرى والتي تنضوي تحت أي من هذين الموضوعين (الملكية الأدبية أو الصناعية) فإن عدد الدول العربية المنضمة قليل جدا، وبالعموم تحتل مصر المركز الأول بين الدول العربية في عدد الاتفاقيات التي انضمت إليها وتبلغ 11 اتفاقية من أصل 24 وقد انضمت مصر إلى اتفاقية التربس عام 1995 [1] ثم المغرب (10 اتفاقيات) فتونس (9 اتفاقيات) ثم الجزائر (8 اتفاقيات) فلبنان (6 اتفاقيات).

ويوضح الجدول 2 تاليا مواقف الدول العربية من اتفاقيات الملكية الفكرية التي ترعاها وتديرها المنظمة العالمية للملكية الفكرية، ويشير إلى سنة انضمام الدولة إلى الاتفاقيات المذكورة، أما بالنسبة لاتفاقية تربس فإن

---

(1) بموجب قرار السيد رئيس الجمهورية رقم 72 لسنة 1995 بانضمام مصر إلي منظمة التجارة العالمية أصبحت اتفاقياتها قانونا محليا ومن هذه الاتفاقيات اتفاقية: أوجه الملكية الفكرية المرتبطة بالتجارة المعروفة اختصارا باسم " تربس ".

عضوية أي من الدول العربية في منظمة التجارة العالمية يجعلها عضوا ملتزما بأحكام هذه الاتفاقية.

ونشير في هذا المقام، إلى أن عضوية الدولة في اتفاقية تربس سيجعلها ملزمة حكما بما أحالت إليه من اتفاقيات في ميدان الملكية الفكرية، وهي بشكل رئيس اتفاقيتا بيرن وباريس إضافة إلى اتفاقية روما واتفاقية واشنطن المتعلقة بالدوائر المتكاملة(طبعا في حدود المواد التي أشارت إليها اتفاقية تربس من بين مواد هذه الاتفاقيات).

كما أن إنفاذ أحكام بعض الاتفاقيات والقوانين الوطنية السائدة في الدولة يطرح بإلحاح وجوب وقوف الدول العربية أمام مختلف هذه الاتفاقيات وبحث مدى الإفادة من العضوية فيها والالتزام بها، إذ ليس كل اتفاقية ترتب بالضرورة التزامات فقط، بل إن جزءا منها يحل مشكلات عملية ويساهم في سلامة نظام الحماية، كما هو الحال بالنسبة لاتفاقيات التصنيف في ميدان العلامات التجارية وعلامات البضائع وغيرها من اتفاقيات الاتحادات الدولية والاتفاقيات الإجرائية والتنظيمية.

ونرى في هذا المقام وجوب خضوع سائر هذه الاتفاقيات للدراسة الشاملة لدى كل دولة بالمقارنة مع نظامها القانوني وما هو مقرر لديها من قواعد تشريعية واستراتيجيات عملية في ميدان الملكية الفكرية لجهة بناء موقف صحيح من العضوية فيها.[1]

وقد شهدت المنطقة العربية مؤخرا جملة من دعاوى الملكية الفكرية بخصوص برامج الحاسوب والتسجيلات الصوتية إضافة إلى عدد من المنازعات في ميدان الألعاب الإلكترونية بمختلف أنواعها، ويعزى النشاط

(1) د.فؤاد جمال: إطلالة على حماية حقوق الملكية الفكرية في مصر، منشور ضمن مجلة "رسالة المعرفة"، مركز تنمية البحوث، المخابرات العامة المصرية، العدد الثاني، 2006. راجع في هذا الموضوع د.جمال عبد الله - ندوة المعلوماتية القانونية والقضائية، المركز العربي للدراسات والبحوث القانونية،1998

المتزايد في هذا الميدان إلى ما تقرر من تفعيل تطبيق قوانين حق المؤلف وإلى نشاط الشركات الأجنبية المترافق مع سياسات تحرير التجارة في السلع والخدمات والوفاء باستحقاقات عضوية منظمة التجارة العالمية.

وقد قضت المحكمة في طعن بخصوص الملكية الفكرية والرقابة على المصنفات أنه لما كانت المادة الخامسة من قانون حماية حق المؤلف رقم 354 سنة 1954 قد نصت على أن للمؤلف وحده الحق في تقرير نشر مصنفه وفي تعيين طريقة هذا النشر. وله وحده الحق في استغلال مصنفه مالياً بأية طريقة من طرق الاستغلال ولا يجوز لغيره مباشرة هذا الحق دون إذن كتابي سابق منه أو ممن يخلفه ".

كما نصت المادة 37 من القانون ذاته على أن: " للمؤلف أن ينقل إلى الغير الحق في مباشرة حقوق الاستغلال المنصوص عليها في المواد 5 " فقرة 1 "، 6، 7 " فقرة 1 " من هذا القانون على أن نقل أحد الحقوق لا يترتب عليه مباشرة حق آخر - ويشترط لتمام التصرف أن يكون مكتوباً وأن يحدد فيه صراحة وبالتفصيل كل حق على حدة يكون محل التصرف مع بيان مداه والغرض منه ومدة الاستغلال ومكانه ".

فإن مفاد ذلك أن المشرع قد حرص على أن يكون للمؤلف وحده الحق في تقرير نشر مصنفه واستغلاله بأية طريقة على ألا يكون لغيره مباشرة حقه في الاستغلال على أية صورة دون الحصول على إذن كتابي سابق منه حال حياته أو ممن يخلفه بعد وفاته، وتعاقب المادة 47 من القانون ذاته على مخالفة ذلك بما نصت عليه من أنه: " يعتبر مكوناً لجريمة التقليد ويعاقب عليه بغرامة لا تقل عن عشرة جنيهات ولا تزيد على مائة جنيه كل من ارتكب أحد الأفعال الآتية: " أولاً " من اعتدى على حقوق المؤلف المنصوص عليها في المواد 5، 6، 7 فقرة أولى وثالثة من هذا القانون. " ثانياً " من باع مصنف مقلد... إلخ " ثالثاً " من قلد في مصر مصنفات.[1]

---

(1) الطعن رقم 0760 لسنة 50 مكتب فني 31 صفحة رقم 899 بتاريخ =

قد يعتقد البعض - خطأ - أن دعاوى الملكية الفكرية حديثة ومستجدة، لكن الحقيقة أنها من الدعاوى القائمة منذ فجر القرن معتمدة على طائفة من التشريعات والاتفاقيات الدولية التي انطلقت مع نهايات القرن التاسع عشر، ففي الأردن مثلا - كما في عدد من الدول العربية المجاورة - ظل قانون حق المؤلف العثماني ساريا اعتبارا من عام 1906 إلى أن تدخلت الدول بوضع تشريعات أكثر شمولية في ضوء موجبات الاتفاقيات الدولية التي تديرها المنظمة العالمية للملكية الفكرية - الوايبو وفي عدد من الدول العربية - كالأردن مثلا تم إلغاء قانون حق التأليف العثماني واستبداله بتشريعات حماية حق المؤلف، وشهدت التسعينات موجة تشريعية واسعة في المنطقة العربية أبرز ملامحها إضافة برامج الكمبيوتر وقواعد البيانات إلى نطاق المصنفات محل الحماية بموجب تشريع حق المؤلف. [1]

بالرغم من انطلاق الجهد الدولي المنظم في حقل تحرير التجارة منذ عام 1947 الذي شهد ولادة اتفاقيات الجات، فإن تحرير التجارة في السلع أصبح يواجه معيقات كبرى أهمها عدم قبول الولايات المتحدة طائفة كبيرة من اتفاقيات تحرير التجارة برغم الجولات التفاوضية السبعة التي سبقت جولة الأورغواي (1986 - 1994) [2]، وفي جولة الأورغواي للتفاوض بشأن تحرير التجارة في السلع، انتقل العالم إلى واقع جديد حين فاجأته الولايات المتحدة بقبول غالبية ما كانت ترفضه من اتفاقيات في حقل تجارة البضائع، ولم يكن هذا الموقف خاليا من رؤية استراتيجية للمصالح الأمريكية في

=16 - 10 - 1980، أحكام نقض في الرقابة على المصنفات متوفر على الرابط:

http://www.f - law.net/law/threads

(1) سميحة القليوبي، "الملكية الصناعية"، دار النهضة العربية، (بدون سنة الطبع)، ص. 37 وأيضاً، محمد حسني عباس، "الملكية الصناعية أو طريق انتقال الدول النامية إلى عصر التكنولوجيا"، المنظمة العالمية للملكية الفكرية، جنيف 1967

(2) Michael Hudson، Super Imperialism: "The Origin and Fundamentals of U.S. World Dominance"، 2nd ed. (London and Sterling، VA: Pluto Press، (2003)، P. 258.

المستقبل، بل هو وليد دراسات وتخطيط استراتيجي ساهمت فيه مختلف الشركات العملاقة متعددة الجنسيات، حيث أقحمت القوى الغربية في جولة الأورغواي - برغم معارضة الدول النامية - موضوع الملكية الفكرية (اتفاقية تربس) وموضوع تحرير التجارة في الخدمات، لجهة خلق واقع جديد يتيح لمالكي المعرفة والكفاءة الإفادة من كافة الأسواق العالمية وتعزيز استثماراتهم فيها، وفعلا تحقق هذا الهدف بإقرار اتفاقية تربس بشأن الملكية الفكرية ليخلق لأول مرة منذ أكثر من مائة عام مركزا آخرا للملكية الفكرية غير المنظمة العالمية (الوايبو) ولتصبح اتفاقية تربس الإطار الأكثر شمولية لمعالجة كافة مسائل الملكية الفكرية.

وأقرت أيضا اتفاقية تحرير الخدمات (جاتس) التي تتيح لمقدمي الخدمة تعاملا مماثلا للجهات الوطنية في الدولة وترفع من أمامهم معيقات الوصول للأسواق الخارجية. وفي هذا الإطار كان يتعين على كل دولة ترغب بعضوية المنظمة أن تقبل هذه الاتفاقيات التي تفرض التزامات تنظيمية وتشريعية من بينها أن تتواءم تشريعاتها في حقل الملكية الفكرية مع اتفاقية تربس.

وفي هذا الإطار شهدت الدول العربية موجة واسعة من تعديل التشريعات القائمة أو وضع تشريعات جديدة، وأحدثت ثورة حقيقة في النظام القانوني للملكية الفكرية في الوطن العربي لا تزال ملامحها غير واضحة، فإذا كانت الخطط المعلنة هي تعزيز الملكية الفكرية لاستجلاب الاستثمار الأجنبي باعتبار ذلك من الأمور المرغبة لجهات الاستثمار وأحيانا من مطالبها، فإن حركة الاستثمارات الأجنبية في الأسواق العربية لا تشير إلى تحقق هذا الغرض بالرغم من أن دولا عربية أقرت تشريعات تحمي الملكية الفكرية أكثر نضجا وشمولية مما هو قائم في دول أجنبية.[1]

وفي الوقت نفسه ظهرت في الواقع العملي ظاهرة نشاط الشركات

(1) محمد واصل، الحماية القانونية للمصنفات الرقمية (برامج الحاسوب) مجلة جامعة دمشق للعلوم الاقتصادية والقانونية - المجلد 27 - العدد الثالث - 2011 ص 18.

الأجنبيـة لتنظيـف الأسـواق العربيـة مـما يسـمونه خطرا عـلى اسـتثماراتها ونقصـد بذلك مـا يثـار حـول مخاطـر القرصنـة، ولم تكتـف هذه الجهـات بالخطـط الحكوميـة الطموحة لتحقيـق هـذا الغـرض، فبـاشرت بذاتهـا حملـة تقـاض - هـي حـق لهـا مـن الوجهـة القانونيـة ومـن وجهـة نظـر العدالـة - مترافقـة مـع حملة تعديـل التشريعـات إلى المدى التـي ظـن البعـض أننـا أمـام تشريعـات جديـدة وأن حمايـة برامـج الحاسـوب انطلقـت مـع هـذه القوانـين، مـع أن الحمايـة مقـررة منـذ نحـو عشرة سـنوات.

الفرع الثالث

النطاق القانوني لحماية برامج الكمبيوتر وقواعد البيانات في البيئة العربية

تتضمن قوانين حماية حق المؤلف العربية عموما النص على حماية الكتب والكتيبات وغيرها من المواد المكتوبة، والمصنفات التي تلقى شفاهة كالمحاضرات والخطب والمواعظ، والمصنفات المسرحية والمسرحيات الغنائية والموسيقية والتمثيل الإيمائي، والمصنفات الموسيقية، والمصنفات السينمائية والإذاعية السمعية والبصرية، وأعمال الرسم والتصوير والنحت والحفر والعمارة والفنون التطبيقية والزخرفية والصور التوضيحية والخرائط والتصميمات والمخططات والأعمال المجسمة المتعلقة بالجغرافيا والخرائط السطحية للأرض، وبرامج الحاسوب (كما في طائفة منها) وفي أعقاب سريان اتفاقية تربس في عدد من الدول العربية أصبحت الحماية تمتد إلى البرمجيات سواء كانت بلغة المصدر أو الآلة، إضافة إلى حماية ما يمكن أن يسمى قواعد المعلومات المجمعة وتحديدا حماية طريقة التجميع سواء كانت بطريقة تقليدية أم آلية (قواعد البيانات). وذلك للتوافق مع متطلبات المادة 10 من اتفاقية تربس العالمية (اتفاقية الجوانب المتصلة بالتجارة من حقوق الملكية الفكرية).[1]

وتحمى برامج الحاسوب وقواعد البيانات وفقا لقوانين حق المؤلف - بوجه عام - طيلة حياة المؤلف ولمدة خمسين عاما بعد وفاته، ويوجه خبراء التقنية والقانون الدوليين انتقادا لمدة الحماية هذه باعتبارها طويلة لا تتناسب مع الطبيعة المتغيرة والمتسارعة للبرمجيات واستغلالها لمدد قصيرة، أما إذا كان مالك حقوق المؤلف شخصا معنويا - وهو الفرض الغالب بالنسبة

(1) فاروق علي حفناوي، قانون البرمجيات، دار الكتاب الحديث،القاهرة،2001.ص65 راجع في الموضوع نفسه: المركز القومي للبحوث الاجتماعية والجنائية، "حق المؤلف والحقوق المجاورة في إطار الملكية الفكرية"، المجلة الجنائية القومية، العدد1،مارس - جويلية1999. ص3.

للبرمجيات، فإن مدة الحماية تقل عن مدة حماية حقوق الأشخاص الطبيعيين كما في عدد من قوانين الدول العربية.

وتشمل الحماية الحقوق المعنوية للمؤلف والحقوق المالية لاستغلال المصنف وهي حماية استثنائية للمؤلف وحده يمنع بموجبها أي استغلال أو استعمال يضر بمصلحة المؤلف، وتعطي للمؤلف وحده الحق في استنساخ مصنفه وإجازة استعماله، وفقا لشرائط تقررها القوانين العربية في هذا الحقل تتصل بمباشرة حقوق المؤلف ونطاق الاستغلال ومحتواه، تنص القوانين أيضا - على تباين بينها - على استثناءات معينة ترد على مباشرة حقوق المؤلف، ولا تعد من قبيل التعدي، مثالها إجازة استخدام المصنف دون إذن المؤلف أو مالك الحق في معرض تقديم المصنف عرضا أو إلقاء خلال اجتماع عائلي أو في مؤسسة تعليمية أو ثقافية أو اجتماعية على سبيل التوضيح أو الاستعانة بالمصنف لأغراض شخصية بعمل نسخة واحدة دون تعارض مع الاستغلال العادي، واستعماله في الإيضاح التعليمي والاستشهاد بفقرات منه في إنتاج ووضع مصنف آخر.[1]

وتجيز بعض القوانين للسلطات إصدار أمر بالترخيص الإجباري للمصنف الأجنبي رغما عن مالكه لجهة وإعادة إنتاجها وبيعها بالسعر المساوي لمثيلاتها في السوق أو السعر العادل ضمن ضوابط وشروط يراعى فيها تعويض مؤلف المصنف أو صاحب الحق عن هذا الترخيص الإجباري. وتتبع الدول طريقة الترخيص الإجباري حماية لاحتياجات المجتمع والعملية التعليمية، وتتباين المواقف حول نطاق الترخيص الإجباري إذ يحدد القانون عادة المصنفات القابلة لمثل هذا الإجراء، وهو أيضا إجراء مهم لمواجهة سياسات الاحتكار ومنعا للتحكم في رواج الفائدة المتوخاة من المصنف.[2]

---

(1) الإطار القانوني الدولي لحماية حق المؤلف والحقوق المجاورة، من وثائق الويبو،وثيقة /WIPO/IP BAH/05/ص42

(2) يوسف احمد النوافلة، الحماية القانونية لحق المؤلف، دار الثقافة للنشر والتوزيع، الأردن، ط2004.ص 56 راجع أيضا محمد حسام لطفي، الحماية القانونية لبرامج الحاسب =

وبسبب الأثر الذي أحدثته اتفاقية تربس، لم يعد شرط إيداع المصنفات مطلوبا لغايات الحماية القضائية، وهو ما أدى إلى تعديل عدد من تشريعات حق المؤلف العربية لتعكس هذا الحكم كما أن التشريعات الحديثة منها نصت أيضا على عدم اشتراط الإيداع.

و لكن هناك قصور في التنظيم القانوني الوطني يتجلى في عدم إعمال المبادئ الأساسية التي تقوم عليها الاتفاقية مثل مبدأ المعاملة الوطنية ووجود قصور في التنظيم القانوني الوطني يتمثل في عدم اعتناق القواعد الاتفاقية الحمائية أو وجود قواعد وطنية تقرر حماية أقل مما ورد في الاتفاقية أو تتعارض معها، وكذلك وجود قصور في التنظيم القضائي يتمثل في عدم مراعاة حقوق الدفاع الأساسية التي أشارت إليها الاتفاقية.

ومن ثم وإذا ثبت وجود قصور متعمد في التنظيم القانوني الوطني يتعلق بحماية حقوق الملكية الفكرية فيعتبر ذلك إخلال بالالتزامات وتتحمل الدولة المسؤولية الدولية.[1]

= الإلكتروني، جامعة بني سويف، 1987.

(1) د.أبو العلا النمر.المرجع السابق.

الفرع الرابع

إشكالات حماية البرمجيات وقواعد البيانات

أولا: محل الحماية:

إن تحديد مفهوم البرنامج ونطاقه خلق إشكاليات عديدة، أولها ما إذا كان إعادة إنتاج البرنامج باقتباس أجزاء منه، أو باستخدام طريقة الهندسة العكسية أو باتباع وسائل برمجية (معنوية) غير المتبعة في إنتاجه أصلا، يعد من قبيل النسخ غير المشروع أو التقليد، ويتفق القضاء على أن التقليد أو النسخ لكامل المنتج بغرض الاستغلال المالي لا يثير إشكالا في التطبيق، لكن ما يثير الإشكال هو اقتباس الخوارزميات المحتواة ضمن البرنامج، ومرد ذلك أن القضاء الأجنبي في معرض نظره لدعاوى حقوق المؤلف على البرمجيات اتسق مع أحكام الاتفاقيات الدولية بشأن عدم شمول الخوارزميات والحقائق للحماية، وهذا ما يعني أن الاقتباس فيما لا يتجاوز النسخ الجزئي وطريقة الهندسة العكسية المتبعة في إعادة بناء البرنامج تخضع لمعايير معينة قبل القول بحصول النسخ أو الاعتداء على حق المؤلف.[1]

ويثور الإشكال أيضا بالنسبة لحماية لغة البرمجة، وتعديلات استخدام برامج التشغيل للتوافق مع بيئات العمل التقني أو لجهة إصلاح أخطائه، ومفهوم أن الشائع في حقل القرصنة بالعموم إنما هو برمجيات التشغيل الشهيرة وبرامج التطبيق الشائعة، لكن الإشكال يثور حول النسخ التجريبية التي يزود بها المستخدمون، فهي ليست المصنف النهائي المثبت ملكيته، ويثبت ذلك بالمعايير الفحصية عبر الخبرة، ومعلوم أن الشائع والسائد في الدول

(1) يونس عرب، الحقائق الخفية في دعاوى الملكية الفكرية، نسخه إلكترونيه،2010 ص134 راجع أيضا صلاح الدين مرسي، الحماية القانونية لحق المؤلف في التشريع الجزائري، رسالة دكتوراه في القانون، كلية الحقوق جامعة بن عكنون، الجزائر، 1988م، ص150.

النامية النسخ التجريبية التي يتلقاها في وقتنا الحاضر معظم المستخدمين عبر شبكة الإنترنت أو حتى من بائع الأجهزة بحصوله عليها من الوسائط التي تملأ العالم ضمن سياسات الترويج الإعلامي التي اتبعتها وتتبعها المؤسسات المنتجة للبرمجيات.[1]

ثانياً:شرط ملكية الحق أساس الدعوى ولا دعوى دون توفر الصفة في التقاضي:

إن حماية أي المصنف توجب أن يثبت الحق بملكيته لطالب الحماية، سواء تعلق إجراء الحماية بالمطالبة المدنية (الدعوى المدنية بشقيها الموضوعي والطلبات المستعجلة) أو الدعوى الجزائية (الشكوى) أو الإجراء الإداري عبر مكتب الحماية. وشرط ثبوت تملك الحق المعنوي أو حق الاستغلال المالي، شرط مصلحة وصفة، بل إنه ابتداء عنصر رئيس لتفعيل عمل نصوص الحماية، بمعنى أنه الشرط الموجب لقبول الدعوى، فلا دعوى دون أن يثبت زاعم الاعتداء أنه المالك الحقيقي والقانوني لحقوق المؤلف على المصنف، وهذه من أكثر الإشكالات التي تواجه دعاوى الملكية الفكرية في الساحة العربية، فالإيداع لم يعد متطلبا وفقا لاتفاقية تربس وقد اعتقدت العديد من الجهات أن ذلك يعفيها من إثبات الملكية أو أنها جهات شهيرة إلى مدى يعرف القاضي أنها المالكة للحق على برنامج ما، وهذا ليس صحيحا، إذ على فرض صحته فإن القاضي لا يحكم بعلمه عوضا عن مباشرة حقوق حماية المصنف التي تتطلب أن تتم وتتم فقط من المؤلف وحده الذي منح حق الدفاع عن مصنفه، وتصبح المشكلة أكثر تعقيدا عندما يتصدى لرفع الدعوى وكيل عن مالك الحق، وما لم تثبت وكالته القانونية بأنه وكيل بالخصومة وبنوع هذه الخصومة فإنه لا وجه لقبول الدعوى ابتداء.[2]

---

(1) خالد مصطفي فهمي: الحماية القانونية لبرامج الحاسب الآلي، الإسكندرية، دار الجامعة الجديدة للنشر، سنة 2005 م ص 108.

(2) محمد الفيومي، مقدمة الحاسبات وتشغيل الحاسبات الصغيرة، الإسكندرية، المكتب الجامعي الحديث، سنة 1998 م. ص 45 راجع في السياق نفسه د.أبو العلا النمر المرجع السابق.

ويشترط أن يثبت ملكية حق الخصومة والتقاضي لمن يباشر دعوى أو طلب الحماية عندما لا يكون هو المؤلف أو المتنازل إليه من المؤلف مباشرة عن حق الاستغلال المالي، أما ذا كان طالب الحماية بالإجراء المعين وكيلا أو موزعا فإنه لا يملك غير المقاضاة المدنية بما تعرض له هو بصفته هذه، لا بما تعرض له مؤلف المصنف أو مالك الحق فيه، لأن نطاق وصحة المطالبة تتحدد بسببها، فإن امتد سبب المطالبة إلى ادعاء الاعتداء على حق المؤلف فهو - أي المؤلف وحده - من يحمي الحق أو من يحق له أن يوكل غيره في الخصومة القضائية لهذه الغاية تحديدا، وكل ذلك مرهون بنصوص عقود واتفاقيات الوكالة والرخص. [1]

وهو ما يدعونا في هذا المقام للتنبيه إلى أن كثيرا من المؤسسات كانت محلا لتعاقدات غير عادلة مع الأطراف الأجنبية بسبب عوامل كثيرة أهمها مدى كفاءة المفاوض، وعدم توفر المشورة القانونية المؤهلة المتخصصة في هذا الحقل المهم.[2]

ثالثاً ترخيص المصنف:

لقد وقعت العديد من الشركات والمؤسسات العربية ضمن نطاق تأثير الموزعين والوكلاء بل وسماسرة السوق، وتعرضوا للإيهام بأن أوضاعهم القانونية مخالفة للقانون مع أن وضعهم القانوني قد يكون سليما ولا غبار عليه، ومثال ذلك اعتبار مؤسسة ما غير مرخصة مع أنها تملك أجهزة حواسيب ذات ماركات عالمية منتجة من شركات عقدت اتفاقيات داخلية مع جهات إنتاج البرامج تعتبر بموجبها أجهزتها مرخصة حكما حتى لو لم

---

(1) لطفي، محمد حسام: الحماية القانونية لبرامج الحاسب الإلكتروني، دار الثقافة للطباعة والنشر، سنة 1978 م. ص 89 راجع أيضا لطفي، محمد حسام: المرجع العلمي في الملكية الأدبية والفنية، سنة 1996 م.

(2) الدعوى الاستئنافية رقم2001/207 الصادر قرارها بتاريخ 2/21 / دليل الأحكام – دار الفكر العربي2001 ص231.

تتحقق معايير الترخيص المقررة لدى جهة إنتاج البرامج ومثال آخر اعتبار حائز التسجيلات التي سبق له شراؤها من أحد الوكلاء السابقين مخالف للقانون لأن وكالة الوكيل التجارية تحظر عليه إبقاء أي مخزون لدى التجار في نهاية مدة وكالته، فيخل بالتزامه ويعرض التجار للمسؤولية أمام الوكيل الجديد الذي لا يفترض غير أن التاجر قد نسخ مصنفاته دون إذن. [1]

ومثال ثالث استغلال عدم معرفة العديد من المؤسسات بأنها مرخصة أصلا لعدم معرفتها بماهية الرخصة ذاتها، وأشير في هذا المقام إلى أن الأسواق العربية تشيع فيها ممارسات من قبل بائعي الأجهزة التقنية (ممارسات السوق) من ضمنها مثلا تنزيل نسخة واحدة من البرنامج على قرص واحد على عدد من الأجهزة رغم أن المشتري كان قد اشترى عددا من البرمجيات المرخصة يساوي عدد الأجهزة، بحيث تظهر كافة الأجهزة محملة برقم البرنامج نفسه فتتعرض لاتهامها بنسخ البرنامج على أجهزتها، مع أن الواقع غير ذلك.

ومن الممارسات أيضا عدم إرسال كتيب الرخص من قبل البائع على اعتبار أنه كتيب تعليمات لتتفاجأ الشركة بعد ذلك أنها غير مرخصة لأنها لم تحضر رخص برمجياتها من البائع الذي يكون قد أودعها مخزنه أو مستودعا ما أو ربما اعتبرها من مخلفات الأجهزة كعبوات التغليف والكتيبات فأتلفها أو ألقاها إلى حيث يلقي مخلفاته غير المهمة. ومثل هذه الممارسة قد تتم من الشركة المشترية التي لا تعير الكتيبات والأدلة والأوراق المصاحبة للجهاز اهتماما كافيا أو لا تعير أهمية للاحتفاظ بالرخص في موضع يمنع فقدها وضياعها. [2]

---

(1) شحادة غريب شلقامي، برامج الحاسب الآلي والقانون، القاهرة، دار النهضة العربية، سنة.2003 ص 109 راجع في السياق ذاته، عباس، محمد حسني، الملكية الصناعية والمحل التجاري، عمان، دار الفرقان، سنة 1994

(2) مدحت محمد محمود عبد العال، مدى خضوع برامج الحاسب الآلي للحماية المقررة للمصنفات، الأدبية في ظل قانون حماية حق المؤلف، القاهرة، دار النهضة العربية، سنة 2002راجع أيضا فهمي، خالد مصطفي: الحماية القانونية لبرامج الحاسب الآلي، =

ومن المخاطر الحقيقة لعدم الوعي السائد بشأن التراخيص استغلال البعض لهذه الممارسات التي لا دخل للمستخدمين فيها بسبب غياب المعايير والمواصفات التقنية وغياب استراتيجيات تنظيم السوق التقني في البيئة العربية، وأوضح مثال على ذلك أن بعض الجهات التقنية تعتبر المستخدم غير مرخص لاستخدام برنامج معين حتى لو أبرز الرخصة المطابقة نوعا وتاريخا للبرنامج لكنها لا تتطابق مع البرنامج من حيث رقم المنتج، إذ قد يختلف رقم البرنامج الموجود على الجهاز مع رقم المنتج الوارد على الرخصة لأسباب كثيرة، منها - كما ذكرنا - أن بعض الجهات تقوم بإنزال البرنامج على عدة أجهزة على قرص واحد لتوفر وقت إنزال كل برنامج من القرص الخاص به وباعتبارها جميعا نسخا متطابقة من البرنامج.

أو قد يتم محو القرص الصلب بكامله لغايات الصيانة أو التطوير فلا تراعي جهة الصيانة تنزيل النسخة الموجودة عند العميل وتنزل من طرفها نسخة من البرنامج ذاته فيختلف الرقم، وقد يختلف الرقم لأي سبب آخر باعتباره من الناحية التقنية قابل للتغيير بتدخل شخصي أو نتيجة عمليات مؤتمتة مما يجعل الرقم مغايرا للرقم الموجود على الرخصة، وهذا لا يعني أن المستخدم غير مرخص له باستخدام البرنامج، لأن رقم المنتج ليس معيارا للترخيص ولا هو متطلب له، والمعيار فقط توفر وثيقة الرخصة ذاتها المطابقة للبرنامج نوعا وتاريخا فقط، إذ لا يعتد بما يقبل التغيير كالرقم، ولا أهمية له ولا دور يقوم به من ناحية الترخيص، وهو موجود فقط لتسهيل عمليات الدعم والصيانة (للمسجلين لدى الشركة المنتجة فقط مع الإشارة إلى أن التسجيل اختياري وليس متطلبا قانونيا لصحة الاستخدام) أو يستخدم الرقم داخل المنشأة لغايات التوثيق وصرف العهدة على المستخدمين عند تعددهم.[1]

= الإسكندرية، دار الجامعة، الجديدة للنشر، سنة 2005 م و كذلك كنعان، نواف: حماية حقوق التأليف لبرامج الحاسبات الإلكترونية، بحث منشور في مجلة الاداره العامة، العدد 59، سنة 1988 م.

(1) لطفي، محمد حسام: الحماية القانونية لبرامج الحاسب الإلكتروني، دار الثقافة للطباعة =

لهذه الممارسات التي نشأت عن تشوه سوق التقنية وغياب المعايير والمواصفات على مدى السنوات السابقة، علينا جميعا أن نعيد التفكير بشعار مكافحة القرصنة الذي يتعين أن يسبقه معرفة حقيقة وسليمة بالواقع المعاش وباستراتيجيات جهات الترخيص والإنتاج، فمن مصلحة المنتج أن يعتبر أي فعل من قبيل الاعتداء على فرص ربحه، لكن من حقنا أيضا أن نعرف ما إذا كان فعلا يعتمد على استراتيجية تتفق والقانون القائم أو أنه يتحدث عن نظامه القانوني واستراتيجياته التي يرغب أن تكون قانونا لكنه لا يملك ذلك في ظل اعتبارات السيادة الوطنية.

إن الاتفاقيات الدولية وبقدر ما منحت المبدع حقوقا على نتاج إبداعه، بقدر ما حمت المستهلك من التضليل والإيهام، وعلينا أن ندرك أن إيفاءنا بالتزاماتنا تجاه الغير - وهو أمر مطلوب ومرغوب لدينا بسبب التركيبة الاجتماعية والثقافة السائدة في مجتمعنا - يتعين أن يرافقه تمسكنا بحقوقنا التي تنطلق أولا من المعرفة والوعي بالحدود الفاصلة بين الحق والالتزام في هذا الحقل.

إن الموضوعية تقتضي منا الإشادة العالية باتجاهات القضاء في هذا الحقل، حيث أظهرت بعض الوقائع العملية أن القضاء يعتمد على نفسه أولا وعلى خبرات فنية يقلبها بعناية للوصول إلى الحقيقة، ففي قرار صادر عن محكمة الاستئناف الأردنية [1] بوصفها المرجع القضائي الأخير للطلبات المستعجلة قضى فيه ببطلان ضبط تسجيلات صوتية، قررت المحكمة إخضاع كافة المضبوطات في ميدان الملكية الفكرية إلى شرائط القانون والحكم بعدم

= والنشر، سنة 1978 م ص 29.

(1) في أول قرار قضائي صادر عن محكمة استئناف عمان في الدعوى رقم 2000/1313 تاريخ 2000/5/18 قضت محكمة الاستئناف الأردنية بفسخ قرار محكمة البداية المستعجل القاضي بمنع التعدي وضبط مصنفات مقلدة من الكاسيت وماكينات التسجيل المستخدمة في التقليد بسند من القول إن مثل هذا القرار دخول في أصل الحق وإصداره يتطلب التأسيس على أدلة كافية لإصداره أولها وأبرزها الخبرة الفنية.

قبول أي ضبط دون خبرة قاطعة بحصول السلوك الجرمي من الشخص المنسوب إليه الفعل بذاته، وينظر القضاء للأمر بكل عناية وموضوعية. وقد أظهرت الدعاوى المنظورة وأخرى من المفصولة حتى الآن اتجاها قضائيا يقوم على تمحيص الحقائق إلى أبعد مدى لتبين الحقائق حول التراخيص سيما في ظل تنوعها وفي ظل ما يعلن على الملأ من إمكان الترخيص اللاحق للبرامج القائمة، بل في ظل صفقات الترخيص المسماة (التواؤم مع متطلبات القانون) فهي – ونحن لسنا ضدها على الإطلاق بل نشجعها - تثير من الوجهة القانونية التساؤل حول بعض الخبرات الفنية التي لا تقبل تراخيص بزعم مخالفتها لمعايير مقررة لدى جهات الترخيص التي هي الشركات الأجنبية المنتجة ذاتها، كالمغايرة بين رقم الرخصة والبرنامج مع أنه غير متطلب ابتداء، والأساس التطابق بين الرخصة ونوع البرنامج وتاريخ تنزيله، فجهات الترخيص عند عقد الصفقات تكيف معاييرها لتمرير صفقاتها التجارية، لكنها في ساحات القضاء قد تتمسك بمعاييرها هي لضمان مركز أفضل أمام القضاء.[1]

ومن هنا فإن كافة الخبراء الفنيين العرب مدعوون للتعامل الدقيق والحذر مع الحالات المكلفين بها، لأن العلم لا يقبل التطويع لحساب سياسات نفعية، والقضاء يبذل كل جهد للوصول إلى الحقائق الموضوعية، ولأن كثيرا من المفاهيم تغيب في أوقات يفترض أن لا تغيب، وكثيرا مما يعتقد أنه حقيقة علمية لا يعدو مجرد سياسة تسويقية لشركة مستفيدة أو منتفعة. [2]

وفي ميدان البرمجيات، تثور مشكلة نطاق التراخيص وحجيتها وأنواعها المستجدة، إذ لم تقف تراخيص التصرف بالبرمجيات واستعمالها عند

---

(1) نبيلة إسماعيل رسلان المسؤولية في مجال المعلومات والشبكات، مجلة روح القوانين، كلية الحقوق، جامعة طنطا، العدد 18، سنة 1999 م ص 20.

(2) Focusing public attention on emerging privacy and civil liberties issues، "Electronic Privacy and Information Center: Choicepoint" P.21. EPIC. Retrieved 2013 - 11 - 19.

حـد الرخصـة المكتوبـة الموقعـة مـن طرفيهـا، بل أصبحـت البرمجيـات تباع كحـزم جاهزة في أماكـن البيـع العـام، تتضمـن رخصـا نموذجيـة غير موقـع عليهـا، توجب التزام مشـتري البرنامـج بشرائطهـا بمجـرد فـض العبـوة ونزع الغـلاف، كما أن مـن البرامـج وتحديدا تلك المشـتراة عـلى الخـط أو المنزلـة والمثبتـة عـبر الشـبكات كالإنترنـت والانترانـت الخاصـة بتسـويق البرمجيـات مـا ترتبـط فيهـا الرخصـة بقبـول الـشروط المكتوبـة والمنشـورة عـلى الموقـع بحيـث يصبـح الشـخص ملزمـا بمحتواهـا بمجـرد القبـول وأحيانـا الاسـتعمال، وبعضهـا تتضمـن الرخصـة بشـكل إلكـتروني ضمـن مقدمـة البرنامـج ذاتـه، مـع مرافقـة ذلـك بإجـراءات تسـجيل تتـم أحيانـا بشـكل مـادي عـلى مسـتنداتها أو بشـكل إلكـتروني عـبر الشـبكة، ولا يترتـب عـلى عـدم القيـام بهـا في حـالات عديـدة آثـار عـلى صحـة الاسـتخدام في حـين أن شروط بعـض الرخـص تربـط صحـة الاسـتخدام بإتمـام التسـجيل، وهـذه الرخـص تثـير إشـكاليات قانونيـة في التطبيـق توجـب التدقيـق في طبيعتهـا والبت بأمـر حجيتهـا في ضـوء أحـكام قانـون البيانـات وتحديـده للأدلـة المقبولـة قانونـا.[1]

إن مشـكلات عـدم الاطـلاع فعليـا عـلى هـذه الـشروط في كثـير مـن الحـالات، مشـكلات عـدم معرفـة قواعـد الإثبـات القائمـة لهـذه الـشروط المخزنـة داخـل النظـم كـشروط نموذجيـة تثبـت عنـاصر والتزامـات التعاقـد، لعـدم التوقيـع عليهـا وعـدم ثبـوت توجيههـا لشـخص بعينـه، وثبـوت عدم مناقشـتها بـين الأطراف، كل ذلك وغيره اسـتوجب التدخـل التشريعـي لتنظيـم آليـة إبـرام العقـد التقنـي أو شروط حجيتـه وموثوقيتـه، سـواء نتحـدث عـن العقـد المتصـل بالمبيـع أو عـن رخـص الاسـتخدام بوصفهـا التزامـا بين جهتين.[2]

وتثـور أيضـا مشـكلة رخـص الملكيـة الفكريـة المغلفـة مـع المبيـع، وكذلـك حقـوق الملكيـة الفكريـة في ميـدان النـشر الإلكـتروني خصوصـا مـع تزايـد

(1) سرور، طارق أحمد: الحماية الجنائية لأسرار الأفراد في مواجهة النشر، رسالة دكتوراه، دار النهضة العربية، القاهرة، سنة 1991 م.ص 67.

(2) أحمد بدر. مجتمع المعلومات الكوني ومشكلات الخصوصية وأمن المعلومات وحق التأليف. - مجلة مكتبة الملك فهد الوطنية. - مج 3، ع 2 1998م) ص 68.

الاستيلاء على التصاميم التي يستخدمها موقع ما، وحقوق الملكية الفكرية على أسماء المواقع، وعلى ملكية الموقع نفسه، وحقوق الملكية الفكرية بالنسبة للعلامات التجارية للسلع، والأسماء التجارية، وكذلك حقوق المؤلفين على محتوى البرمجيات التقنية التي تنزل على الخط أو تسوق عبر مواقع التجارة الإلكترونية.

إن أبرز مشكلات التعامل مع الرخص غياب المعرفة بأنماطها وتحديد مدى الصحة من عدمه ولعل هذا ما دعا مختلف الدول العربية لعقد عشرات البرامج التوعوية والتدريبية في حقل التراخيص، وقد أظهرت هذه البرامج حقائق مذهلة حتى بالنسبة للخبراء الذين لم يسبق لهم معرفتها، وهذا يضع مجتمعنا وكل الجهات العاملة في حقل الملكية الفكرية في تحد علينا تجاوزه بكل فعالية، وهو التأهيل الصحيح البعيد عن الغرض لموضوع التراخيص منطلقين من حاجة الوطن ومؤسساته لبناء نظام تراخيص تفاوضي ومعرفي وقانوني وتنظيمي فيه الصالح الوطني عمادا وعنوانا.

رابعاً: ثبوت أركان الجرم على نحو ما حدده القانون فقط وبدليل مشروع

مما يثار في حقل إشكالات الدعاوى الجزائية المتعلقة بالملكية الفكرية، المفاهيم العامة التي تطلق في الاتهام أحيانا وحتى في الدفاع من قبل بعض جهات الدفاع، كالقول إن الدعوى تقوم على فعل مخالف لقانون حق المؤلف في حين أن القانون الجزائي لا يعمل وفق هذه العمومية المرفوضة بموجب مبدأ المشروعية، وإلا لكنا نحيل السارق والقاتل والمزور بتهمة واحدة وهي مخالفة قانون العقوبات.[1]

إن دعاوى المساءلة الجزائية في حقل الملكية الفكرية، تخضع شأنها شأن غيرها لقواعد المشروعية الجنائية ويتعين أن تثبت عناصر الجرم وفقا لنموذجه

(1) أحمد فضل شبلول. حول الملكية الفكرية وحقوق المؤلف على شبكة الإنترنت، 2007. متاح في:
http://www.meo.tv/culture/?id44632

القانوني فقط، وتخضع أيضا من حيث إثبات المسؤولية لمبدأ مشروعية الدليل من حيث مصدره وانتفاء احتمالات الشبهة والغاية فيمن يعتمد عليه لإثبات الجرم. ولا تثبت كافة العناصر وكذا لا تقبل الأدلة على سبيل الاحتمال، وإنما على سبيل الجزم واليقين شأنها شأن غيرها من الدعاوى الجزائية ويتعين أن يحدد مرتكبها دون شك، لأن المسؤولية الجزائية شخصية، ولأن نطاق مسؤولية الأشخاص المعنوية توجب إثبات قيام ممثل الشخص المعنوي قانونا أو من في حكمه بارتكاب الجرم المتوفر فيه كافة الأركان المقررة قانونا، المادي والمعنوي ووفق النموذج القانوني المحدد في نص التجريم.[(1)]

إن القضاء المقارن قد قرر وجوب ثبوت تحقق الاستنساخ أو التقليد بمعنى ثبوت مقارفة السلوك المادي المكون للجريمة وفق ما نص عليه القانون، وبشكل لا يظهر منه أن محل النسخ واحدة من عمليات الاقتباس أو ما عرف بنسق الهندسة العكسية في بيئة إنتاج البرمجيات، وهذه مسائل تتطلب الخبرة القانونية والفنية، وهي لجدتها في ميدان التقاضي تثير عشرات الدفوع والمسائل الفرعية التي سيكون للخبرة فيها دورا حاسما وأساسيا، مع التأكيد أن الخبير الأعلى إنما هو القاضي، وهو الذي يحكم في المواد الجزائية بقناعته الذاتية ووجدانه المستقى والمستخلص على نحو سائغ من أدلة الدعوى.

إن محكمة الاستئناف الأردنية وفي أحدث أحكامها [(2)] في ميدان دعاوى المسؤولية عن قرصنة برامج الكمبيوتر، حللت بكل دقة وعمق النصوص الجنائية المقررة في قانون حق المؤلف الأردني، وتوصلت بوضوح إلى أن الأنشطة المجرمة في هذا الحقل تنحصر بأنشطة الاستغلال المالي المتمثلة بالعرض للبيع أو التأجير وفي حدود غرض محدد فقط وهو الاستغلال المالي، ومن هنا قررت بوضوح أن الاستخدام دون الاستغلال المالي لا يعد جرما

(1) عبد الصادق، محمد سامي: حقوق مؤلفي المصنفات المشتركة، رسالة دكتوراه، جامعة القاهرة، سنة 2000 م. ص 189.

(2) الدعوى الاستئنافية رقم2001/207 الصادر قرارها بتاريخ 2/21 / 2001 - الأردن متوفر www.arblaw.com

وفق القانون، وأنهت نهاية موضوعية وعادلة واحدة من دعاوى الملكية الفكرية التي طالت واحدة من المؤسسات المالية الكبرى، ولا نبالغ إن قلنا إن حماية الإبداع بكل صورة في ميدان الملكية الأدبية والصناعية قام على أساس الموازنة بين احتياجات المبدع لصيانة إبداعه ومنحه الفرصة (المؤقتة بمدة معينة) لاستثمار نتاج عقله، وبين حاجة المجتمع للمعرفة ووسائلها، هذه الموازنة التي تمنع احتكار صاحب المصنف لمصنفه، وتجيز ترخيصه إجباريا لحماية الثقافة وتلبية احتياجات التنمية والتطور في المجتمع. وإذا كان من حق مالك حقوق أي مصنف أن يحمي إبداعه، فإن من حق مجتمعنا علينا أن لا تكون هذه الحماية على نحو يمس عناصر تطوره ويخل بميزان التناسب بين الحماية الخاصة والاحتياجات الجماعية.

الفرع الخامس

دور المشرع المصري

لمّ يكن التشريع المصري غائباً عن الاهتمام بحماية حقوق المؤلف في العصر الرقمي، وانطلاقاً من هذا الواقع بدأت مراجعة التشريعات الوطنية القائمة وتطويرها للوفاء بالالتزامات الدولية وتوفير الحماية اللازمة للمجالات الجديدة التي يتعين أن تمتد إليها الحماية.

ومن ثمَّ فقد قام المشرع المصري بإعداد تشريعاً موحداً يعالج جميع جوانب الملكية الفكرية، وقد عالج القانون رقم 2003/88 بشأن حماية حقوق الملكية الفكرية في أربعة كتب، واستناداً لهذه الحماية صدرت اللائحة التنفيذية لهذا القانون، والموضحة على النحو التالي:

الكتاب الأول: يعالج براءات الاختراع ونماذج المنفعة التصميمات التخطيطية للدوائر المتكاملة والمعلومات غير المفصح عنها.

الكتاب الثاني: تناول العلامات والبيانات التجارية والمؤشرات الجغرافية والرسومات والنماذج الصناعية.

الكتاب الثالث: حقوق المؤلف والحقوق المجاورة.

الكتاب الرابع: وموضوعه الأصناف النباتية.

كما نصت المادة الثانية من القانون رقم 38 لسنة 1992 بتعديل قانون حماية حق المؤلف على أن تشمل الحماية مصنفات الحاسب الآلي من برامج وقواعد بيانات وما يماثلها من مصنفات تحدد بقرار من وزير الثقافة.

وقد صدر قرار وزير الثقافة رقم 82 لسنة 1993 بتنفيذ قانون حماية حق المؤلف فيما يتعلق بمصنفات الحاسب الآلي والذي عرّف برنامج الحاسب بأنه: مجموعة تعليمات معبر عنها بأي لغة أو رمز ومتخذة أي شكل

مـن الأشـكال يمكـن اسـتخدامها بطريـق مبـاشر أو غـير مبـاشر في حاسـب لأداء وظيفـة أو الوصـول إلى نتيجـة سـواء كانـت هـذه التعليـمات في شـكلها الأصـلي أو في أي شـكل آخـر تتحـول إليـه بواسـطة الحاسـب.

وقـد أورد القانـون رقـم 29 لسـنة 1994 بتعديـل قانـون حمايـة حـق المؤلـف الحكـم نفسـه مضيفـا إليـه هـذه الفقـرة: "وتعتـبر هـذه المصنفـات مـن المصنفـات الأدبيـة"، وهـو المنحـى ذاتـه الـذي اتخـذه المشروع المعـد بمعرفـة وزارة العـدل بقانـون حمايـة حقـوق الملكيـة الفكريـة، وذلـك في الكتـاب الثالـث الخـاص بحقـوق المؤلـف والحقـوق المجـاورة.

كـما أنشـئ بمقتـضى القـرار الوزاري 58 لسـنة 1997 جهـاز نقطة الاتصال لشـؤون حمايـة حقـوق الملكيـة الفكريـة وذلـك تنفيـذا لالتزامـات مـصر لانضمامهـا لاتفاقيـة جوانـب التجـارة المتصلـة بحقـوق الملكيـة الفكريـة (TRIPS) ومـا تقرره المـادة 69 منها مـن التـزام الـدول الأعضـاء في منظمـة التجـارة العالميـة بإنشـاء نقـاط اتصـال (Focal Point) لتبـادل المعلومـات مـع نقـاط الاتصال الأخرى بشـأن التجـارة في السـلع المتعدية لحقـوق الملكيـة الفكريـة. ولقـد أعيـد تشـكيل جهـاز النقطـة بمقتضى قرار وزيـر التجارة الخارجيـة رقـم 379 لسـنة 2001 الـذي نـص عـلى الأنشـطة التـي للنقطـة أن تباشرهـا، وتتمثـل أهـداف الجهـاز فيـما يلي:

- تبـادل المعلومـات مـع نقاط الاتصال الأخرى المنشـأة في البلدان الأعضاء.
- معاونـة السـلطات الجمركيـة المصرية فيما يتعلـق بالتدابير الحدودية.
- التعـاون مـع الجهـات المعنيـة في إجـراءات منـع التعـدي عـلى حقـوق الملكيـة الفكريـة الـواردة بالاتفاقيـة وإرشـاد أصحـاب الشـأن في كيفيـة الحفـاظ عـلى حقوقهـم.
- تلقـــى وفحـــص الشـــكوى والموضوعـــات المقدمـــة للجهـــاز ودراســـتها

والتحقق من صحتها وذلك بالتنسيق والتعاون مع الجهات المختصة وفقاً للقانون والاتفاقيات الدولية وإبداء الرأي فيها.

- عرض التسوية الودية والتوفيق بين الطرفين المتنازعين بناءً على رغبتهما.

- التعاون مع الأجهزة المعنية في نشر المعلومات والتعريف والتوعية بحقوق الملكية الفكرية من خلال التنسيق والعمل والمشاركة في المؤتمرات والندوات والتدريب وورش العمل محلياً ودولياً.

ويحظر قانون حماية حق المؤلف أي نسخ كلى أو جزئي للبرنامج أو الاقتباس منه إلا بعد الحصول على ترخيص كتابي مسبق من صاحب حق المؤلف، كما يحظر تداول أي برنامج مقلد أو منسوخ سواء أتم جلبه من الخارج أو تم تصديره للخارج. وتضمنت العقوبات الواردة على مخالفة هذه الأحكام الحبس والغرامة.

و قد اهتم المشرع المصري بحماية البرمجيات والملكية الفكرية وأصدر:

- قانون حماية الملكية الفكرية رقم 82 لسنة 2002، والذي ينظم حقوق المؤلف وبراءات الاختراع والرسوم والنماذج الصناعية والعلامات التجارية والدوائر المتكاملة وحماية أصناف النباتات.

- اختصاص الهيئة بحماية برامج الحاسب وقواعد البيانات بمقتضى قانون تنظيم التوقيع الإلكتروني وإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات رقم 15 لسنة 2004.

- إنشاء مكتب حماية الملكية الفكرية لمصنفات الحاسب الآلي بهيئة تنمية صناعة تكنولوجيا المعلومات.

- قرار السيد وزير الاتصالات والمعلومات رقم 107 لسنة 2005، بتفويض كل من السيد الرئيس التنفيذي للهيئة ومدير مكتب الحماية بمباشرة وتنفيذ أحكام القانون.

- تعديل جدول الرسوم الملحق باللائحة التنفيذية للقانون والصادرة بقرار السيد رئيس مجلس الوزراء رقم 2202 لسنة 2006.

و قد حرصت مصر على الانضمام إلى الاتفاقيات والمعاهدات الدولية المتعلقة بحقوق الملكية الفكرية، وذلك استناداً إلى أهمية حقوق الملكية الفكرية في حفز الابتكار والإبداع في مصر وجذب مزيد من الاستثمارات الأجنبية.

- الاتفاقيات الدولية التي انضمت لها مصر تنحصر فيما يلي:
- معاهدة باريس لحماية حقوق الملكية الصناعية لعام 1883.
- معاهدة برن لحماية المصنفات الأدبية والفنية لعام 1886.
- اتفاق مدريد بشأن التسجيل الدولي للعلامات لعام 1891.
- اتفاق مدريد لقمع بيانات مصدر السلع الزائفة والمضللة لعام 1891.
- اتفاق لاهاي بشأن الإيداع الدولي للرسوم والنماذج الصناعية لعام 1925.
- اتفاقية ستراسبورج بشأن التصنيف الدولي للبراءات لعام 1971.
- معاهدة واشنطن بشأن الملكية الفكرية فيما يختص بالدوائر المتكاملة لعام 1989.
- معاهدة قانون العلامات التجارية لعام 1994.
- وأخيراً اتفاقية جوانب التجارة المتصلة بحقوق الملكية الفكرية trips الملحقة باتفاقية إنشاء منظمة التجارة العالمية ملحق (1/ج)، وهي اتفاقية تلزم أعضاءها بتطبيق مبدأ الدولة الأولى بالرعاية والمعاملة الوطنية، حيث أصبح لكل أجنبي الحق في أن يعامل في مصر معاملة الوطني بغض النظر عن معاملة دولته لرعاياها.

كذلك أصبح من حق أي دولة عضو من الدول الأعضاء في منظمة التجارة العالمية الاستفادة من أي مزايا تحصل عليها أي دولة من مصر، وفي المقابل يتمتع رعايا مصر بالحقوق ذاتها في مواجهة الدول الأعضاء في المنظمة.

المبحث الثاني

تاريخ القوانين التي تحكم خصوصية البيانات في القوانين المقارنة

بعد مناقشة الإطار العام لتشريعات الخصوصية وجب البحث في:

- تاريخ القوانين التي تحكم الخصوصية في القوانين المقارنة مثل القانون الأمريكي (**المطلب الأول**).
- وكذلك المملكة المتحدة (**المطلب الثاني**).

المطلب الأول

إطار تشريعات الخصوصية في الولايات المتحدة

لا تحظى خصوصية البيانات بالتشريع أو التنظيم المطلوب في الولايات المتحدة. ففي الولايات المتحدة، يتاح الدخول على البيانات الشخصية التي تحتويها تقارير الائتمان لطرف ثالث على سبيل المثال عند تعيين الأفراد أو تقديم الرعاية الطبية أو تقديم قروض السيارات أو الإسكان أو غير ذلك من المشتريات التي تسدد قيمتها وفقا لشروط الائتمان.

وعلى الرغم من توافر لوائح جزئية، فإنه ليس هنا قانون شامل ينظم الحصول على البيانات الشخصية وتخزينها واستخدامها في الولايات المتحدة. وبشكل عام، أي شخص يبذل جهدا في الحصول على البيانات يكون له حق تخزينها واستخدامها حتى إذا ما تم جمع البيانات دون تصريح.[1]

فعلى سبيل المثال، نجد أن قانون إخضاع التأمين الصحي لقابلية النقل والمحاسبة لسنة 1996 Health Insurance Portability & Accountability Act وقانون حماية خصوصية الأطفال على الإنترنت لسنة 1998 Children's Online Privacy Protection Act وقانون المعاملات الائتمانية العادلة والدقيقة لسنة 2003 Fair & Accurate Credit Transactions Act كلها تعد أمثلة للقوانين الأمريكية الفيدرالية التي تحوى نصوصا تميل إلى تشجيع كفاءات تدفق المعلومات.

ولقد فسرت المحكمة العليا الدستور بأنه يمنح حق الخصوصية للأفراد في القضية المرفوعة من جريسوالد - المدير التنفيذي لاتحاد تنظيم

(1) Marc Rotenberg، and Paul M. Schwartz Privacy، Information، and Technology، Aspen Publishers، 2007pp30

الأسرة - ضد ولاية وكونيكتيكات. ومع ذلك، نجد عددا قليلا للغاية من الولايات التي تقر بأحقية الفرد في الخصوصية باستثناء ولاية كاليفورنيا. فهناك حق للخصوصية غير قابل للتصرف فيه في المادة 1 من القسم الأول من دستور كاليفورنيا كما أن المجلس التشريعي قام بسن عدد من التشريعات التي استهدفت حماية هذا الحق.

ويطالب قانون حماية الخصوصية الإلكترونية لسنة 2003 Online Privacy Protection Act من مشغلي المواقع التجارية أو الخدمات الإلكترونية والتي تقوم بجمع معلومات شخصية حول سكان كاليفورنيا من خلال المواقع الإلكترونية أن تضع وبشكل واضح سياسة للخصوصية privacy policy على الموقع وأن تلتزم بتلك السياسة.[1]

ولقد وضعت وزارة التجارة الأمريكية ترتيب الملاذ الآمن لأجل توفير وسيلة للشركات الأمريكية تستعرض بها التزامها بتوجيهات المفوضية الأوروبية وبذلك تبسط العلاقات بينهم وبين التجارة الأوروبية.[2]

ولقد قام مؤخرا واضعو القوانين باقتراح تشريعات لتغيير الطريقة التي تتعامل بها التجارة الإلكترونية معلومات المستخدمين.

ومن بين تلك التشريعات التي حظيت باهتمام بارز عدد من تشريعات عدم التتبع Do Not Track legislations وقانون حق المعرفة Right to Know Act. ولسوف يطالب قانون الحق في المعرفة لولاية كاليفورنيا في حالة تمريره من كل عمل تجاري يحتفظ بمعلومات عن المستخدمين أن يزود مستخدميه بنسخة من المعلومات المخزنة عند طلبها.

(1) William Prosser "Privacy"، California Law Review (Vol 48، No. 3، (1990) pages 383 - 423)

(2) Puzis Rami، Yagil Dana، Elovici Yuval، and Braha Dan (2009). "Collaborative Attack on Internet Users› Anonymity." Internet Research 2012 p 60 - 77.

ولقد واجه مشروع القانون Bill معارضات شديدة من المجموعات التجارية التي تمثل شركات مثل جوجل ومايكروسوفت وفيس بوك مما أدى إلى عدم إقراره.[1]

- و قد اعتمدت الولايات المتحدة الأمريكية على فكره القوانين القطاعية والتي تحكم قطاع معين في مسألة الخصوصية وهذا ما سنتناوله في **(الفرع الأول)**.
- ثم نتناول التسلسل التاريخي لقوانين الخصوصية في الأفرع التالية بداية بقانون الخصوصية لعام **1974(الفرع الثاني)**.
- ثم قانون خصوصية الاتصالات الإلكترونية لسنة 1986**(الفرع الثالث)**.
- و بعد ذلك قانون حماية خصوصية المستهلك لعام 1997**(الفرع الرابع)**.
- ثم قانون حماية خصوصية الضمان الاجتماعي على الخط لعام 1997 **(الفرع الخامس)**.
- وقانون خصوصية الاتصالات لعام 1997**(الفرع السادس)**.
- وبعد ذلك قانون الخصوصية الشخصية على الإنترنت لسنة 2001 و2002 **(الفرع السابع)**.
- وأخيرا قانون تحديث قانون الخصوصية لمواكبة عصر المعلومات لسنة 2011**(الفرع الثامن)**.

(1) Tynan، Dan. "Real names، real problems: Pseudonymity under siege." ITWorld.، 2013.p 13

الفرع الأول

القوانين القطاعية التي تنظم مفهوم الخصوصية

أولاً: قانـون إخضاع التأمين الصحي لقابلية النقل والمحاسـبة (HIPAA)

قـام مجلـس النـواب الأمريـكي بسـن قانون إخضـاع التأمين الصحـي لقابليـة النقل والمحاسـبة Health Insurance Portability & Accountability Act في عـام 1996 وقـد عـرف هـذا القانـون أيضـا بقانـون كنـدي - كاسـيبون لإخضـاع التأمـين الصحـي لقابليـة النقـل والمحاسـبة، ووضـع موضـع التنفيـذ في 21 أغسـطس 1996. والفكـرة الرئيسـة لقانـون إخضـاع التأمـين الصحـي لقابليـة النقـل والمحاسـبة هـي أنـه يجـب على الفـرد الـذي يخضـع لعمليـة التعـرف الفرديـة عـلى المعلومـات الصحيـة أن:

- تتوافـر لديـه إجـراءات معمـول بهـا لممارسـة حقـوق خصوصيـة المعلومـات الصحيـة الفرديـة.
- يكـون الاسـتخدام والإفصـاح عـن المعلومـات الصحيـة الفرديـة مـصرح بـه أو مطلـوب.[1]

ومـن الصعوبـات التـي تواجـه قانـون إخضـاع التأمـين الصحـي لقابليـة النقـل والمحاسـبة هـي أنـه لا بـد مـن وجـود آليـة لاعتـماد المريـض الـذي يطلـب الدخـول على بياناتـه / بياناتهـا.

ونتيجـة لذلـك، بـدأت المرافـق الطبيـة في السـؤال عـن رقـم الضـمان الاجتماعـي مـن المـرضى، وبذلـك يمكـن القـول بأنـه قـد تـم خفـض الخصوصيـة مـن خـلال تبسـيط إجـراء ربـط السـجلات الطبيـة بالسـجلات الأخـرى.

---

(1) Wolf M، Bennett C. "Local perspective of the impact of the HIPAA privacy rule on research". Cancer،(2006) P.57.

وتمثل قضية الحصول على الموافقة مشكلة وفقا لقانون إخضاع التأمين الصحي لقابلية النقل والمحاسبة وذلك لأن مقدمي الخدمات الطبية يجعلون الرعاية مشروطة بالموافقة على معايير الخصوصية المعمول بها.(1)

ثانياً: قانون الإبلاغ عن الائتمان العادل (FCRA).

يطبق قانون الإبلاغ عن الائتمان العادل Fair Credit Reporting Act (وهو قانون فيدرالي ينظم جمع ونشر واستخدام المعلومات الخاصة بالمستهلكين بما في ذلك المعلومات المتعلقة بالحسابات الائتمانية للمستهلكين) مبادئ قانون الممارسة العادلة للمعلومات لوكالات الإبلاغ عن عمليات الائتمان.(2)

ووفقا لقانون المعاملات الائتمانية العادلة والدقيقة Fair & Accurate Credit Transactions Act، فإنه يمكن لكل شخص الحصول على تقرير سنوي مجاني عن وضعه الائتماني free annual credit report.(3)

ولقد كان قانون الإبلاغ عن الائتمان العادل فعالا في منع انتشار ما يطلق عليه بالأدلة (جمع دليل) الخاصية المزيفة لمعاملات الائتمان. وكانت الأدلة الخاصة بمعاملات الائتمان تقدم فيما سبق معلومات تفصيلية - غير موثوق بها - حول الأفراد المتميزين. وقبل صدور قانون الإبلاغ عن الائتمان

(1) Atchinson، Brian K.; Fox، Daniel M "The Politics Of The Health Insurance Portability And Accountability Act". Health Affairs 1997 P146-150.

(2) Cooper، Marion B.; Drinker Biddle & Reath LLP "January 1، 2013: New Fair Credit Reporting Act "FCRA" Forms Required by New Enforcement Agency". TNL Review.، 2013.p 93 Cite uses deprecated parameters (help)

(3) Singletary، Michelle "Somewhat More Fair And Increasingly Accurate". The Washington Post (2003 - 12 - 11) P.13

العادل كان بالإمكان تضمين مواد بذيئة لا أساس لها، وفي الحقيقة كان يتم تضمين الشائعات بشكل واسع في تقارير الائتمان. ويضم تحالف صناعة النشر الإلكترونية Electronic Publishing Industry Coalition صفحة لقانون الإبلاغ عن الائتمان العادل. كما أن لجمعية صناعة بيانات المستهلكين والتي تمثل صناعة الإبلاغ عن المستهلكين موقع على الإنترنت يحوي معلومات عن قانون الإبلاغ عن الائتمان العادل.[1]

ويزود قانون الإبلاغ عن الائتمان العادل المستهلكين بالقدرة على مراجعة وتصحيح ومعارضة والحد من استخدامات تقارير الائتمان. كما يقوم قانون الإبلاغ عن الائتمان العادل بحماية وكالة الائتمان من تهمة النشر بطريقة مهملة في حالة إذا ما ادعى الطالب تحريف البيانات.

وعلى وكالات الائتمان مطالبة طالب البيانات بتحديد الغرض من نشر المعلومات المطلوبة، إلا أن عليها ألا تبذل جهدا في التحقق من صحة تأكيدات طالب المعلومات. وفي الحقيقة، حكمت المحكمة بأن: " القانون لا يقدم علاجا لاستخدام المعلومات الخاصة بالمستهلكين بشكل غير مشروع أو ضار"، (قضية هنري ضد فوربس عام 1976). ومن السائد أنه لأجل تجنب قانون الإبلاغ عن الائتمان العادل، قامت أكويفاكس Equivax بإنشاء تشويس بوينت ChoicePoint وفي ذلك الوقت قامت الشركة الأم بنسخ كل سجلاتها ونقلتها إلى شركتها التابعة الحديثة التأسيس. وتشويس بوينت ليست بوكالة الإبلاغ عن الائتمان، وبالتالي فإن قانون الإبلاغ عن الائتمان العادل لا ينطبق عليها.

ويحد قانون الممارسات العادلة في استرداد الديون Fair Debt Collection Practices Act بالمثل من نشر معلومات حول المعاملات

---

(1) Rumbaugh، Eric H.; Jason A. Kunschke; Michael Best & Friedrich LLP "Fair Credit Reporting Act Background Checks Remain a Hot Topic for Employers". The National Law Review. 2013.

المالية للمستهلك. فهو يمنع الدائنين أو وكلائهم من كشف حقيقة أن فرد مدين لطرف ثالث برغم أنه يسمح للدائنين ووكلائهم بمحاولة الحصول على معلومات حول موقع المدين. وهو يحد من تصرفات هؤلاء الذين يسعون إلى تسديد دين.

فعلى سبيل المثال، يحظر على وكالات استرداد الديون من مضايقة أو الاتصال بالأفراد في مواقع عملهم. ويحد قانون منع انتهاكات الإفلاس وحماية المستهلك Bankruptcy Abuse Prevention & Consumer Protection Act والصادر في عام 2005 (والذي دعم سبل حماية المستهلك كما على سبيل المثال في حالة الإفلاس الناجم عن ارتفاع التكاليف الطبية) من بعض هذه القيود المفروضة على المدينين.[1]

في الولايات المتحدة، تغطي القوانين الإضافية النوعيات المختلفة من المعلومات الخاصة. فعلى سبيل المثال، يطالب قانون الحقوق التعليمية والخصوصية العائلية Family Educational Rights & Privacy Act والذي تم سنه في عام 1974 الوالدين أو الطالب الراشد بالموافقة على الدخول على سجلات الطلاب لمعظم الأغراض.[2]

ولدى العديد من الوكالات الفيدرالية الأمريكية قوانين خصوصية تغطي عملية جمعها واستخدامها للمعلومات الخاصة. ومن هذه الوكالات، مكتب الإحصاء الرسمي للسكان، وكالة خدمة العائدات الداخلية والمركز القومي لإحصائيات التعليم (تحت قانون إصلاح العلوم التعليمية).

---

(1) Paul A.JMistakes Do Happen: A Look at Errors in Consumer Credit Reports". United States Public Interest Research Group. Archived from the original on 2006 P 98

(2) Mendelsohn، Stephen A.. "U.S. Department of Education Amends its FERPA Regulations to Allow for Certain Additional Student Disclosures". The National Law Review. 2012 P 59

وبالإضافة إلى ذلك، يحمي قانون حماية المعلومات السرية والكفاءة الإحصائية Confidential Information Protection & Statistical Efficiency Act (CIPSEA) سرية البيانات التي يتم تجمعيها من وكالات الإحصاء الفيدرالية.[1]

وعلى نقيض المفهوم الأمريكي لحماية الخصوصية والذي يعتمد على التشريع المعني بالصناعة والتنظيم والتنظيم الذاتي، يعتمد الاتحاد الأوروبي على تشريع شامل للخصوصية.

ويشمل التوجيه الأوروبي حول حماية البيانات European Directive on Data Protection والذي بدأ العمل به في أكتوبر 1998 على سبيل المثال الاحتياج إلى إنشاء وكالات حماية البيانات الحكومية وتسجيل قواعد البيانات لدى تلك الوكالات وفي بعض الأحيان وقبل الموافقة على بدء معالجة البيانات الشخصية.

ولأجل عبور مفاهيم الخصوصية المختلفة هذه وتوفير وسائل سلسلة للهيئات الأمريكية كي تلتزم بالتوجيه، وضعت وزارة التجارة بالتشاور مع المفوضية الأوروبية إطارا للـ"الملاذ الآمن safe harbor". والملاذ الآمن الذي اعتمده الاتحاد الأوروبي في يوليو من عام 2000، هو وسيلة للشركات الأمريكية كي تلتزم بالخصوصية الأوروبية.

(1) CIPSEA Report on confidentiality and data sharing from the U.S. Energy Information Administration retrieved from www.eia.gov 2013

الفرع الثاني

قانون الخصوصية لعام 1974

تـم سـن قانـون الخصوصية لعـام 1974 – القانون العام رقم 93 - 59 – اسـتجابة للمخـاوف حـول الكيفيـة التـي يمكـن أن يؤثـر بهـا إنشـاء واسـتخدام قواعـد البيانـات المميكنـة عـلى حقـوق الخصوصيـة للأفراد.

أولا: طالـب القانـون الـوكالات الحكوميـة تعرض عـلى الأفراد أي سـجلات تحتفظ بهـا عنـه أو عنهـا. ويضمـن القانـون الخصوصيـة مـن خـلال إنشـاء أربعـة حقـوق إجرائيـة ورئيسـة في البيانات الشـخصية.

ثانيـا: طالـب القانـون الـوكالات بإتبـاع مبـادئ معينـة يطلـق عليهـا الممارسـات العادلـة للمعلومـات "fair information practices" عنـد جمـع ومعالجـة البيانـات الشـخصية.

ثالثـا: يفـرض القانـون قيـودا عـلى الكيفيـة التـي يمكـن بهـا للـوكالات مشـاركة بيانـات الأفـراد مـع أفـراد آخريـن أو وكالات أخـرى.

رابعـا وأخـيرا: يتيـح القانون للأفـراد مقاضـاة الحكومـة لانتهاكها نصـوص قوانينها provisions.[1]

ومـع ذلـك، هنـاك عـدد مـن الاسـتثناءات لقانـون الخصوصيـة. فالـوكالات الحكوميـة التـي تعمـل عـلى تطبيـق القانـون يمكنهـا أن تعفـي نفسـها مـن قواعـد

---

(1) Report US Secretary›s Advisory Committee on Automated Personal Data Systems، Records، Computers and the Rights of Citizens، Chapter IV: Recommended Safeguards for Administrative Personal Data Systems (1973).

القانـون. كـما أن الـوكالات قـد تحايلـت عـلى قواعـد مشـاركة المعلومـات باسـتغلال اسـتثناء "الاسـتخدام الروتينـي".[1]

في مسـار عمـل الحكومـة الفيدراليـة اليومـي، كان بالـضرورة أن تحتفـظ بمئـات مـن قواعـد البيانـات حـول الأفـراد. ومـع تقـدم التكنولوجيـا خـلال عقـدي السـتينات والسـبعينات، أصبـح مـن اليسـير للـوكالات أن تتبـادل بيانـات الأفـراد الشـخصية. وبـدأ المواطنـون والمشرعـون في تدبـر السـبل التـي يمكـن بهـا انتهـاك هـذه المعلومـات إذا مـا تـم جمعهـا. ومـع قـدرة الحاسـبات الآليـة عـلى البحـث عـبر الملفـات المشـتركة بسرعـة ويـسر، وكان جليـا أن التفصيـلات المختلفـة لحيـاة الفـرد يمكـن أن يتـم جمعهـا في قاعدة بيانـات واحـدة.

وفي عـام 1973، أصـدرت إدارة الصحـة والتعليـم والرفاهيـة Department of Health، Education & Welfare (HEW) تقريـرا أطلقـت عليـه: "السـجلات والحاسـبات الآليـة وحقـوق المواطنـين Records، Computers & the Rights of Citizens".[2]

وقـد أوصى هـذا التقريـر بأن يسـن مجلس النـواب تشريعا يطبق قانون الممارسـة العادلـة للمعلومـات لأنظمـة البيانات الشـخصية المميكنة.

ويشـمل هذا القانون المبـادئ التالية:

- يجـب ألا يكـون هنـاك نظـام لحفـظ سـجلات البيانـات الشـخصية يكـون وجـوده محاطا بالسريـة.
- يجـب أن يكـون هنـاك وسيلة يكتشـف بهـا الفـرد ماهيـة المعلومـات التـي تخصـه متوافـرة في السـجلات، والكيفيـة التـي يتـم بهـا اسـتخدام هـذه المعلومـات.

---

(1) The President's Annual Report on the Agencies' Implementation of the Privacy Act of 1974،" CY 1982 - 1983، at 118 (Dec. 4، 1985) P.56.

(2) Mark E L.Engaging Privacy and Information Technology in a Digital Age National Research Council of the National Academies، " (2007).P 83

- يجب أن تكون هناك وسيلة تمكن الفرد من منع المعلومات التي يتم الحصول عليها بشأنه لأحد الأغراض من أن يتم استخدامها أو أن تصبح متاحة لأغراض أخرى دون موافقته.

- لابد من أن تكون هناك وسيلة للفرد تمكنه من تصحيح أو تعديل السجل بشأن معلومات محددة بشأنه.

- وعلى أي هيئة تقوم بإنشاء أو الاحتفاظ أو استخدام أو نشر سجلات البيانات الشخصية المحددة أن تؤكد مصداقية استخدام البيانات للغرض المنتوي منه وعليها أن تأخذ الاحتياطات اللازمة لمنع سوء استخدام هذه البيانات.[1]

كما وضع تقرير الصحة والتعليم والرفاهية أيضا توصيات محددة بشأن القوانين التي سيتم بتنفيذ وتفعيل هذا القانون.

وطالب هذه التوصيات الهيئات التي تحتفظ بقواعد بيانات مميكنة حول الأفراد من أن:

(1) تسن الضمانات التي تؤمن هذه البيانات.

و(2) تبلغ العامة كل عام ماهية قواعد البيانات التي تحتفظ بها ونوعية المعلومات التي بحوزتها.

كما حدد تقرير الصحة والتعليم والرفاهية أيضا قائمة بالحقوق التي يتوجب أن يحظى بها الأفراد "موضوع البيانات" (الأفراد الذين تم تخزين بياناتهم الشخصية). ولقد أصبح الكثير من هذه التوصيات في النهاية جزءا من قانون الخصوصية الصادر في عام 1974.[2]

---

(1) Report of the Secretary›s Advisory Committee on Automated Personal Data Systems U.S. Department of Health، Education & Welfare OHEW Publication NO. (OS) July (1973) P.73

(2) Wilson J "Health Insurance Portability and Accountability Act Privacy rule causes ongoing concerns among clinicians and researchers". Ann Intern Med (2006). P.145.

ولقد قام تقرير الصحة والتعليم والرفاهية أيضا بدراسة مستفيضة لقضية رقم الضمان الاجتماعي (Social Security Number (SSN. وكان ذلك يمثل اهتماما محددا نظرا لأن رقم الضمان الاجتماعي بدا أنه يمثل المرشح الأكثر احتمالا لإنشاء "المحدد المعياري العام (Standard Universal Identifier (SUI والذي يمكن استخدامه كأساس لربط كافة السجلات التي تحتفظ بها كافة الوكالات حول شخص ما .

وبالنظر إلى هذه المخاطر، أوصى تقرير الصحة والتعليم والرفاهية أن يتم استخدام رقم الضمان الاجتماعي فقط متى كان لذلك ضرورة قصوى (كما على سبيل المثال، استخدام إدارة الضمان الاجتماعي له من أجل منح مميزات أو أينما تطالب القوانين المعمول بها من الوكالات باستخدام رقم الضمان الاجتماعي)، وأنه لا يحق لأي وكالة أن تنشر أرقام الضمان الاجتماعي الموجودة بحوزتها ما لم يدعو مجلس النواب إلى ذلك على وجه التحديد. ولقد كانت هذه التوصيات بارزة أيضا في النص النهائي لقانون الخصوصية.[1]

تم وضع قانون الخصوصية ليكون بمثابة تسوية بين مشروعي القانونين المنفصلين، تم تقديم أحدهما في مجلس النواب، والأخر في مجلس الشيوخ.[2]

ويميل مشروع قانون مجلس الشيوخ - S. 3418 - إلى أن يحوى متطلبات أكثر تشددا للحكومة عما يميل إليه مشروع قانون مجلس النواب

---

(1) B، Eagle K "Potential impact of the HIPAA privacy rule on data collection in a registry of patients with acute coronary syndrome". Arch Intern Med P165 (2005).

(2) Kirsch، Michael S"Alternative Sanctions and the Federal Tax Law: Symbols، Shaming، and Social Norm Management as a Substitute for Effective Tax Policy". Iowa Law Review. (2004). P 89

حيث تضمن عقوبات أكثر تشددا لعمليات انتهاك القانون[1] وكذلك إنشاء مفوضية حماية الخصوصية Privacy Protection Commission للإشراف على تنفيذ القانون. كما تطلب مشروع قانون مجلس النواب رقم H.R. 16373 أيضا اعتبار عمليات انتهاك محددة للقانون أن تكون "متعمدة willful أو استبدادية arbitrary أو نزوية capricious" قبل أن يتم تقييم الأضرار ضد الحكومة في حين يكتفي مشروع قانون مجلس الشيوخ بانتهاك القانون. ولقد نظر الجهازان كلاهما في مشروعي القانون المختلفين في وقت متأخر من الجلسة ثم قررا توفيق اللغة في اجتماع غير رسمي بين فريقي عمل من مجلس النواب ومجلس الشيوخ. ومن بين عمليات التوفيق الرئيسة ما يلي:

إنشاء مفوضية دراسة حماية الخصوصية Privacy Protection Study Commission والتي لن يكون لها سلطة تفعيل العقوبات على انتهاكات القانون وإنما عوضا عن ذلك، سوف تقدم التوصيات المتعلقة بمزيد من عمليات التنفيذ ومن تفعيل القانون.[2]

لابد وأن بعض عمليات الانتهاك الحكومية المحددة وأن تكون "متعمدة أو مقصودة" من أجل إيقاع الأضرار بأحد الأفراد. ولقد تم الاعتقاد بان ذلك يعد حملا أكثر يسرا للفرد المشتكي عن كونها " متعمدة أو استبدادية أو نزوية"، وإن كانت أكثر شدة من مجرد إظهارها بأنها انتهاك للقانون.

يتم ضمان حصول المشتكين "المستحقين للتعويض" على مبلغ ألف دولار عن الأضرار، تم تضمين استثناء "الاستخدام الروتيني routine use" لمجلس النواب لمشاركة المعلومات.

---

(1) U.S. Department of Justice، "Office of Privacy and Civil Liberties"، Overview of the Privacy Act of 1974 P.23.

(2) Robert Gellman، Fair Information Practices: A Basic History WDC Pub.، 2008P 26.

تـم تضمـين نـص مجلـس الشـيوخ بأنـه بإمـكان اسـتئناف الفـرد لرفـض تعديـل سـجل أمـام محكمـة المقاطعـة الفيدراليـة.

وفقـت هـذه التغـيرات إلى جانـب عـدة تغـيرات أخـرى بـين مشروعـي القانـون ومـع التغيـيرات النهائيـة التـي وضعهـا مجلـس الشـيوخ، قـام مجلـس النـواب بإقـرار القانـون في 17 ديسـمبر واعتمـده مجلـس الشـيوخ في 18 ديسـمبر. ووقـع الرئيـس فـورد عـلى قانـون الخصوصيـة مـع حلـول العـام الجديـد.

وقـد دعـا القانـون إلى إنشـاء مفوضيـة دراسـة حمايـة الخصوصية والتـي أصدرت تقريرهـا حـول الخصوصيـة في عـام 1977. ولقـد اسـتخلص هـذا التقريـر المعنـون "الخصوصيـة الشـخصية في مجتمع المعلومات Personal Privacy in an Information Society" إلى أنـه في حـين كان قانـون الخصوصيـة لسـنة 1974 يعـد خطـوة كبـيرة إلى الأمـام،[1] إلا أنـه يـؤدي إلى الفوائـد التي انتواهـا مجلـس النـواب.

فقـد شـعرت مفوضيـة دراسـة حمايـة الخصوصيـة أن كثـيرا مـن نصـوص أو لغـة language قانـون الخصوصيـة غـير واضحـة، وأن الارتـكان إلى تعريـف "نظـم السـجلات systems of records" كان يمثـل مشـكلة ذلـك لأن تعريـف "تظم السـجلات" قد تضمن فقـط قواعـد البيانـات تلـك التـي تسـترجع المعلومات بالاسـم أو رقم الضـمان الاجتماعي أو غـير ذلـك مـن معلومـات التعريـف الفرديـة.

وبذلــك، فــإن قاعــدة البيانــات التــي تحــوي اســم الفــرد ورقــم الضــمان الاجتماعـي الخـاص بـه قـد لا يغطيهـا قانـون الخصوصيـة ذلـك لأنـه لم يتـم فهرسـتها بالاسـم أو رقـم الضـمان الاجتماعـي أو.... إلـخ. فعـلى سـبيل المثـال، للتحايـل عـلى متطلبــات قانــون الخصوصيــة، قامــت بعــض الــوكالات بإنشــاء قواعــد بيانــات

(1) Report Privacy Protection Study Commission، Personal Privacy in an Information Society Congress press (July 1977).

للعاملين تقوم بتصنيف الأفراد وفقا لرتبهم rank عن تصنيفهم برقم الضمان الاجتماعي أو بالاسم.[1]

ولقد وجدت المفوضية أيضا أن نشر قواعد البيانات في السجل الفيدرالي كان مفيدا برغم من تأثيره المحدود نظرا لأن جمهور عامة القراء للسجل الفيدرالي لم يكن متسعا على وجه الخصوص. كما قالت مفوضية دراسة حماية الخصوصية إن المعلومات التي تقوم الوكالات بالإفصاح عنها في نشراتها غالبا ما تفتقر لتفصيلات مثل الكيفية التي تقوم بها الوكالات باستخدام الأنظمة داخليا.

وفيما يتعلق بدخول الأفراد على البيانات، وجدت المفوضية أن عددا قليلا للغاية من الأفراد قد استفادوا من نصوص قانون الخصوصية للدخول على المعلومات خلال السنوات التي تلت إقرار القانون.

وقد عزت ذلك القصور إلى الافتقار للوعي بنصوص قانون الخصوصية (قياسا بحرية قانون تداول المعلومات Freedom of Information Act المشهور)[2] وللاستثناءات الكاسحة الممنوحة لوكالة المخابرات المركزية ووكالات تطبيق القانون الرئيسة الأخرى.

كما تعرضت الوكالات للنقد لعدم تطبيقها معايير ثابتة لقياس مدى الالتزام بالقانون إذ غالبا ما يسئ كثير من أفراد الطبقة المتوسطة والطبقة الدنيا فهم تعبيرات القانون ويستشهدون بشكل غير مناسب بها كسبب لحجب المعلومات عن الأفراد.

على نقيض قانون حرية المعلومات، يغطي قانون الخصوصية فقط

(1) Robert Gellman، Does Privacy Law Work?، Technology and Privacy: "The New Landscape" n.d p.132

(2) Metcalfe، Daniel J. "The Presidential Executive Order on the Freedom of Information Act"(PDF). 4th International Conferene of Information Commissioners. (23 May 2006) p.54

المواطنون الأمريكيون والمقيمون في الولايات المتحدة بصفة دائمة. وبذلك، يستفيد فقط المواطن والمقيم بصفة دائمة من قانون الخصوصية.

وبالإضافة إلى ذلك، ينطبق القانون فقط على وكالات حكومية فيدرالية محددة (باستثناء القسم السابع من القانون والذي يفرض قيودا على رقم الضمان الاجتماعي والذي ينطبق على الحكومات الفيدرالية وحكومات الولاية والحكومات المحلية).

وبعيدا عن القسم السابع، لا يغطي قانون الخصوصية حكومات الولاية والحكومات المحلية على الرغم من أن الولايات المتفردة لديها القوانين الخاصة بها والمتعلقة بالاحتفاظ بسجلات الأفراد.

بينما يغطي القانون جميع الإدارات التنفيذية والعسكرية والوكالات التنظيمية المستقلة والشركات التي تسيطر عليها الحكومة. وهو ما يعني أن الشركات التي تسيطر عليها الحكومة مثل شركة الخدمات البريدية الأمريكية يجب أن يتم تغطيتها إلى جانب الوكالات العسكرية والتنفيذية مثل إدارة التربية والتعليم وإدارة الغذاء والدواء الأمريكية ومكتب التحقيقات الفيدرالي على سبيل المثال لا الحصر.

ولا يندرج تحت هذا التعريف مجلس النواب برغم أن مكتب الرئيس يندرج تحت هذا التعريف.

وقد وضع القانون عدة أسس في حماية البيانات الشخصية وهي كالتالي:

أولاً: متطلبات الإشعار العام:

وغالبا ما يشير القانون إلى "نظم السجلات"، ويتم تعريف نظام السجلات بأنه: أي مجموعة من السجلات يتم منها استدعاء المعلومات باسم الفرد أو مفتاح تعريف identifier. أما قواعد البيانات ومجموعات السجلات التي لا تسمح باستدعاء معلومات حول فرد بعينه فهي غير مشمولة.

لأجل منع وجود قواعد بيانات سرية، يتوجب على الوكالات نشر تفصيلات كافة أنظمة سجلاتها في السجل الفيدرالي. ويجب أن يغطي الإعلان الاستخدامات المرجوة من النظام، وأن يسمح للأفراد المعنيين بتقديم بيانات مكتوبة أو وجهات النظر أو منازعاتهم arguments إلى الوكالة.[1]

وفي أي وقت ترغب فيه الوكالة إنشاء أو إجراء تغيير بارز في نظام السجلات، عليها أيضا أن تخطر مقدما اللجنة المعنية بالعمليات الحكومية Government Operations بمجلس النواب واللجنة المعنية بالشؤون الحكومية في مجلس الشيوخ ومكتب الإدارة والميزانية Office of Management & Budget. ولسوف تقوم هذه الأجهزة بتقييم التأثير المحتمل أو الكامن على حقوق الأفراد.

ولقد أبطل القانون العام رقم 104 - 66 وقانون إلغاء التقارير الفيدرالية Federal Reports Elimination & Sunset Act لسنة 1995 نصوصا مهمة تطالب الرئيس بتقديم تقرير كل عامين على متابعته لقانون الخصوصية.

ثانياً:الدخول على السجلات:

ويطالب قانون الخصوصية أي وكالة تحتفظ بنظام للسجلات أن تتيح للفرد الدخول على أي سجلات تتعلق به. ويجب أن يتم السماح له بمراجعة السجل والحصول على نسخة منه. وإذا كان السجل غير كامل أو به خطأ، فإنه يحق للفرد أيضا أن يطلب تصحيح هذا السجل. وعلى الوكالة أن تستجيب لهذا الطلب خلال عشرة أيام عمل سواء بإجراء التغييرات المطلوبة أو بإبلاغ الفرد بسبب رفض تغيير السجل. ثم أن على الوكالة أن تخبر الفرد من يخاطبه إذا ما أراد مراجعة الرفض مع مسؤول أعلى رتبة.

---

(1) Scott، Craig R."HIPAA Privacy Complaint Turns Into Federal Criminal Prosecution for First Time". Compliance Corner (University of Missouri Healthcare) 2012

فإذا ما قرر الفرد الاستئناف، فإن لدى الوكالة ثلاثين يوم عمل لمراجعة الرفض. ويمكن للوكالة أن تمد حد الثلاثين يوما ولكن "لأسباب وجيهة ثابتة" فقط.

فإذا ما ظلت الوكالة على قرارها بعد المراجعة بعدم تغيير السجل، يمكن للفرد أن يتقدم بعريضة يوضح فيها سبب اعتراضه على رفض الوكالة. وعلى الوكالة أن تضم تلك العريضة مع أي نسخة من السجل الذي تكشف عنها من ذلك الحين فصاعدا. والوكالة مطالبة أيضا بإبلاغ الفرد بما عليه القيام به لتحويل القضية إلى المحكمة.

ثالثاً: متطلبات كشف الحكومة للمعلومات.

ويقيد القسم الفرعي (ب) من قانون الخصوصية قدرة الوكالة الحكومية على كشف المعلومات القائمة في نظام سجلاتها. ويجوز للوكالة أن تكشف فقط عن المعلومات إذا ما رخص الفرد للوكالة ذلك، أو إذا ما استوفت الوكالة واحدا من الاثني عشر شرطا التالية:

1. عملية الكشف تخص أحد موظفي الوكالة، والذي يحتفظ بشكل طبيعي بالسجل ويحتاجه في أداء واجباته.
2. تتم عملية الكشف وفقا لقانون حرية المعلومات.
3. عملية الكشف هي "للاستخدام الروتيني".
4. عملية الكشف هي لأجل مكتب الإحصاء السكاني، وأغراض عمليات المسح السكاني.
5. عملية الكشف تتم لشخص ما قام بإخطار الوكالة سلفا وباتباع الإجراءات المعمول بها بأنه سوف يستخدم السجل في أبحاث إحصائية، ويتم في هذه الحالة تحويل السجل له دون البيانات المحددة للأفراد.

6. عملية الكشف لإدارة الأرشيف والسجلات القومية كسجل ذي قيمة تاريخية.

7. عملية الكشف لوكالة لها أي صلاحية حكومية داخل أو تحت إشراف الولايات المتحدة لأجل تنفيذ نشاط متعلق بتنفيذ القانون المدني أو الجنائي.

8. عملية الكشف تتم لوجود "ظروف اضطرارية" تؤثر على صحة أو سلامة شخص ما على أن يتم إرسال إخطار إلى الشخص المعرضة صحته أو سلامته لهذه الظروف.

9. عملية الكشف لمجلس النواب أو أي من اللجان أو اللجان الفرعية داخل مجلس النواب.

10. عملية الكشف تتم للمراقب العام في إطار تنفيذ واجباته بمكتب الحسابات العمومي.

11. عملية الكشف تتم وفقا لطلب المحكمة.

12. عملية الكشف تتم لوكالة إبلاغ المستهلكين consumer reporting agency وفقا للقرار رقم 31 U.S.C. 3711(e)

رابعاً: طرق التدقيق Audit Trails.

ينص القسم الفرعي (ج) على ضرورة أن تحتفظ أي وكالة بحسابات دقيقة تبين متى ولمن تم كشف السجلات الشخصية وتشمل معلومات الاتصال الخاص بالشخص أو الوكالة التي طلبت السجلات الشخصية.

ويجب الاحتفاظ بهذه الحسابات لمدة خمسة أعوام أو على مدى حياة السجل أيهما أطول. وما لم يكن مشاركة السجل لأغراض تطبيق القانون، فإن حسابات عمليات الكشف عنها يجب أن تكون متاحة للبيانات محل الطلب.

خامساً: متطلبات تقنين البيانات.

على أي وكالة أن تحتفظ بأدنى قدر من المعلومات "المعنية والضرورية" لتحقيق أغراضها. فإذا ما كان محتملا أن تكون للمعلومات التي يتم جمعها أثر معاكس على الفرد (بتقليص حقوقه أو مصالحه أو امتيازاته)، فإنه يتوجب على الوكالة أن تجمع أكبر قدر من البيانات يمكنها الحصول عليها من الناحية العملية من الفرد ذاته.

وعند جمع هذه المعلومات من الفرد، على الوكالة أن تخطر الفرد ماهية القانون أو الأمر التنفيذي الذي يخول للوكالة جمع المعلومات، والاستخدامات الروتينية التي قد تفيد فيها البيانات والآثار التي من المحتمل أن تنجم نتيجة امتناع الفرد عن تزويد المعلومات المطلوبة.[1]

سادساً: حماية حقوق التعديل الأول First Amendment Rights

لا يمكن للوكالات الاحتفاظ بأي سجلات "تصف الكيفية التي يمارس الفرد بها الحقوق التي يضمنها التعديل الأول" ما لم (1) يصرح قانون منفصل للوكالة بالاحتفاظ بالسجلات، أو (2) يصرح الفرد للوكالة بالاحتفاظ بالسجلات، أو (3) أن يرتبط الاحتفاظ بالسجلات أو يكون في إطار مجال نشاط تطبيق القانون".

سابعاً: حدود مشاركة الوكالة للهيئات الأخرى بالبيانات

أحد أهم سمات قانون الخصوصية أنه يقيد مشاركة المعلومات بين الوكالات الحكومية.

وهو يقوم بذلك بتقييد "برامج المطابقة matching programs" والتي تعرفها بأنها مقارنة إليكترونية لقواعد البيانات لأجل تقرير حالة

---

(1) Harry A. Hammitt، David L. Sobel، and Mark S. Zaid eds.،"Litigation Under the Federal Open Government Laws"(2002) p.71

أو حقوق أو مصالح الأفراد المدرجين في أنظمة السجلات تلك. ويمكن استخدام برامج المطابقة لتبادل المعلومات بين الوكالات الفيدرالية أو بين وكالة فيدرالية ووكالة غير فيدرالية (تذكر أن في نص قانون الخصوصية، فإن كلمة "وكالة" تعني دائما وتقريبا وكالة فيدرالية. إلا أن النصوص التي تقييد برامج المطابقة تنطبق على الوكالات غير الفيدرالية بالمثل).[1]

ويمنع قانون الخصوصية الوكالات من تشغيل برامج المطابقة على نظم السجلات ما لم يكن هناك اتفاق مكتوب بين الوكالات. ويجب عرض هذه الاتفاقية على لجنة الشؤون الحكومية بمجلس الشيوخ ولجنة مراقبة عمليات الحكومة Committee on Government Operations بمجلس النواب كما يجب أن تكون متاحة للعامة أيضا. ويمكن أن تدوم هذه الاتفاقية لمدة 18 شهرا برغم إمكانية تجديدها كل عام طالما لم يقع عليها أي تغيير. ويجب الإبلاغ عن أي تغييرات على نحو الحال مع استخدام نظام جديد للسجلات. ويجب أن تحدد اتفاقية المطابقة ما يلي:

1. الغرض والسلطة القانونية المجيزة لاستخدام برنامج المطابقة.
2. المبرر من استخدام البرنامج ونتائجه المرتقبة بما في ذلك تقدير لأي مدخرات.
3. وصف للسجلات التي سيتم مطابقتها بما في كل عنصر بيانات مستخدم والعدد التقريبي للسجلات المطلوب مطابقتها وتواريخ بداية ونهاية تطبيق برنامج المطابقة المرتقبة.
4. الإجراءات المتنوعة لأجل إشعار الأفراد المحتمل تأثرهم باستخدام البرنامج.
5. التحقق من دقة نتائج البرنامج.

---

(1) Marcia Coyle، Fretting over U.S. data collection: Critics see a lack of privacy protections، National Law Journal، (June 2، 2003) P.1

6. الاحتفاظ بسجلات محدثة ومؤمنة.

7. تنظيم استخدام نتائج أي تقييمات حول مدى دقة السجلات المستخدمة.

8. إضافة قسم يسمح للمراقب العام بالاطلاع على جميع السجلات متى كان ذلك ضروريا لأجل مراقبة الالتزام بتطبيق بنود الاتفاقية.

فإذا ما اعتقدت الوكالة التي تشارك بالمعلومات (الوكالة المصدر) أن الوكالة المتلقية للمعلومات لا تلتزم بكل اللوائح الضرورية، فإنه لا يمكنها كشف أي سجلات للوكالة المتلقية، أو يتم تجديد اتفاقية المطابقة ما لم تشهد الوكالة المتلقية بأنها قد التزمت بكل نصوص اتفاقية المطابقة ولا يكون لدى الوكالة المصدر أي سبب يجعلها تعتقد بأن هذه الشهادة غير دقيقة[1].

يجب على كل وكالة تستخدم برنامج المطابقة أن يكون لديها مجلس استقامة البيانات Data Integrity Board والذي يتكون من كبار المسؤولين بالوكالة بما في ذلك المفتش العام بالوكالة (إن وجد) وأي مسؤول يتم اختياره لمراقبة الالتزام بقانون الخصوصية. وعلى مجلس استقامة البيانات مراجعة واعتماد كل اتفاقيات مطابقة البيانات للتأكد من أن الوكالة ملتزمة بكافة القوانين والتوجيهات على أن يتم تقديم نتائج هذه المراجعة في تقرير سنوي إلى مكتب الإدارة والميزانية كما أنه يجب أيضا إتاحة هذا التقرير للعامة عند طلب ذلك. وعلى المجلس أيضا التحقق من دقة واكتمال المعلومات ومصداقية السجلات. وتمتد سلطة مجلس استقامة البيانات إلى أي من أنشطة المطابقة بالوكالة وليس فقط التحقق من برامج التطابق.[2]

فإذا ما رفض مجلس استقامة البيانات السماح باتفاقية مطابقة مقترحة،

(1) Randall Edwards، Report: Privacy compliance is uneven، Federal Computer Week، (July 30، 2003) p.10.

(2) Kirk Makin،"Ontario court paves way for victims of privacy intrusion to sue snoopers". Globe and Mai (2012 - 01 - 19) p.63

فيمكـن لأي مـن الوكالتـين اللتـين تدعـوان إلى إبـرام الاتفاقيـة الطعـن ضـد هـذا الرفـض لـدى مديـر مكتـب الإدارة والميزانيـة.

ثامناً: عقوبـات انتهاك القانـون: الطعون المدنية Civil Remedies.

يفـرض قانـون الخصوصيـة كلا مـن العقوبـات المدنيـة والجنائيـة عـلى عمليـات انتهـاك أقسـام معينـة. فـإذا مـا رفضـت الوكالـة تعديـل سـجل أحـد الأفـراد بنـاء عـلى الطلـب، يمكـن للفـرد أن يرفـع قضيـة في محكمـة مدنيـة لتمكنـه مـن تعديـل سـجله. وفي هـذه الحالـة، يمكـن للمحكمـة أيضـا أن تحكـم للفـرد برسـوم مناسـبة للمحامـاة وغيرهـا مـن تكاليـف رفـع الدعـوى تقـوم الولايـات المتحـدة بتسـديدها.

وإذا مـا رفضـت الوكالـة السـماح للفـرد بالدخـول عـلى سـجلاته عـلى نحـو ما هو مطلـوب في القسـم الفرعـي (د)(1)، يمكـن للفـرد أن يرفـع قضيـة في محكمـة مدنيـة للمطالبـة بالحصـول عـلى نسـخة مـن سـجلاته. ولسـوف يكـون للمحكمـة التـي تنظـر في هـذه القضيـة القـدرة عـلى مراجعة السـجلات "بشـكل سري" للنظر فيـما إذا كان مطالبة الوكالـة بالسـماح لهـا بأحـد الاسـتثناءات صحيحـا أو لا. ويمكـن أيضـا للمحكمـة أن تلـزم الولايـات المتحـدة بتسـديد رسـوم محامـاة مناسـبة.

فـإذا مـا انتهكـت وكالـة أي قسـم آخر مـن قانـون الخصوصية، ووجـدت المحكمة أن عمليـة الانتهـاك "مقصـودة أو متعمـدة"، فـإن بإمـكان المحكمـة أن تلـزم الولايـات المتحـدة بتسـديد الأضرار الفعليـة التـي تعـرض لهـا الفـرض نتيجـة لعمليـة الانتهـاك (إلا أنـه لـن يتلقـى الفـرد المسـتحق للتعويـض بـأي حـال مبلغـا يقـل عـن ألـف دولار) إلى جانـب تكاليـف ورسـوم المحامـاة المناسـبة.[1]

---

(1) Cathy Beagan Flood، Iris Fischer، Nicole Henderson and Pei Li. "Ontario Court of Appeal Recognizes New Privacy Tort". Blake، Cassels & Graydon p.142

تاسعاً: عقوبات انتهاك قانون الخصوصية: العقوبات الجنائية

إذا ما كشف أي مسؤول أو موظف في وكالة حكومية عن قصد وعمد معلومات تعريف شخصية فسوف يكون مدانا بجنحة ويغرم بمبلغ أقصاه خمسة آلاف دولار. وبالمثل، يمكن تغريم أي موظف أو مسؤول حكومي يحتفظ عن عمد بنظام سجلات دون الكشف عن وجوده والتفصيلات المعنية به على نحو ما سبق توضيحه، بمبلغ أقصاه خمسة آلاف دولار. ويمكن أن تنطبق عقوبة الجنحة نفسها (والغرامة القصوى البالغة خمسة آلاف دولار) على أي شخص يطلب عن قصد وعمد سجل أحد الأفراد من إحدى الوكالات بإدعاء مزيف.[1]

عاشراً: إشراف مكتب الإدارة والميزانية

يمنح قانون الخصوصية مدير مكتب الإدارة والميزانية Office of Management & Budget (OMB) سلطة وضع اللوائح والخطوط الإرشادية بشأن الكيفية التي يتوجب بها على الوكالات تنفيذ القانون. وبذلك، فإن تفسيرات مكتب الإدارة والميزانية للغة قانون الخصوصية تحد قدرا كبيرا من السلطة hold a great deal of authority.[2]

الحادي عشر: قيود على استخدام رقم الضمان الاجتماعي

يشير القسم السابع من قانون الخصوصية إلى أنه ليس بإمكان أي وكالة حكومية فيدرالية أو تابعة للولاية أو حكومية أن تطلب من شخص ما الكشف عن رقم ضمانه الاجتماعي من أجل أن يحصل الفرد على أي حق أو مصلحة أو ميزة يقضي بها القانون. ومع ذلك، لا ينطبق هذا القسم على

---

(1) Geal RF،Federal Trade Commission، Fair Information Practice Principles،(FIPs) review 2009 P 30،

(2) Report، THE PRIVACY ACT AND PERSONALLY IDENTIFIABLE INFORMATION U.S. Department of State Foreign Affairs Manual Volume 5 Information Management p 10 - 15

أي عملية كشف لبيانات أو معلومات "تطلبها القانون الفيدرالي federal statute" أو المعلومات أو البيانات التي يتم استخدامها في نظام سجلات قائم قبل الأول من يناير 1975. ومتى طلبت وكالة حكومية الكشف عن رقم الضمان الاجتماعي، فإن عليها إبلاغ الفرد ما إذا كانت عملية الكشف هذه إلزامية أو اختيارية وأي القوانين يمنح الوكالة سلطة طلب رقم الضمان الاجتماعي والكيفية التي سيتم بها استخدام الرقم.[1]

الثاني عشر: استثناءات قانون الخصوصية

بقدر ما يسعى قانون الخصوصية إلى حماية خصوصية الأفراد، فإن به عددا من الاستثناءات. وهذه الاستثناءات (إلى جانب الصعوبات العملية التي تتضمنها عملية حفظ وتنظيم نظام قواعد البيانات الضخم هذا) تعني أن خصوصية الفرد ليست في أغلب الأحيان تحظى بالحماية الحريصة التي كان يطمح فيها من الذين قاموا بصياغة قانون الخصوصية.

وحيث إن تعريف "السجلات" و"نظم السجلات" و"الوكالات" تعريفا محدودا، نجد أن القانون قد لا يغطي نوعيات كثيرة من قواعد البيانات وأنشطة جمع البيانات. وأخيرا، يسمح استثناء "الاستخدام الروتيني" للوكالات الحكومية أن تكشف معلومات تعريف عن الأفراد وذلك ببساطة بتحديدها لخططها لكشف هذه النوعية من المعلومات عند إنشاء أو تغيير قاعدة البيانات.[2]

الثالث عشر:"السجلات" و"نظم السجلات"

يعرف قانون الخصوصية "السجل" بأنه: أي نوع من المعلومات التي تتضمن اسم الشخص أو تحدد رقمه أو رمزه أو أي خاصية تعريفية تخص

---

(1) Harold C. Relyea، Privacy Protection: Mandating New Arrangements to Implement and Assess Federal Privacy Policy and Practice (CRS Report RS21851) (May 27، 2004)

(2) http://www.privcom.gc.ca/speech/archive/02_05_a_000128_e.asp

الفرد مثل: بصمة أصبع أو بصمة صوت أو صورة". وفي حين كان من الصعب للغاية في عام 1974 التأثير على خصوصية شخص ما دون معرفة اسمه أو رقم ضمانه الاجتماعي أو شكله، فإن تطور قواعد بيانات اليوم تيسر كثيرا التعرف على فرد من مجموعة من الحقائق لا تعد أي منها في ذاتها "خاصية تعريفية identifying particular".[1]

كما يقيد القانون أيضا "نظم السجلات" على "مجموعات السجلات تلك "والتي يتم منها استدعاء المعلومات باسم الفرد أو بأي رقم أو رمز تعريف له أو خاصية تعريفية محددة للفرد".

وكما أشارت مفوضية دراسة حماية الخصوصية، التي تحوي كثيرا من قواعد البيانات معلومات تعريفية شخصية ولكنها لا تستدعي السجلات بتلك المعلومات. وأيا من مثل قواعد البيانات هذه سوف يتم استثناؤها من نصوص قانون الخصوصية بالرغم من احتمال احتوائها على نفس المعلومات، وقد يستمر استخدامها بالطريقة نفسها التي يتم بها استخدام "نظام السجلات" المعترف بها رسميا.[2]

الرابع عشر:أغراض تطبيق القانون

وتتناثر الاستثناءات من "أغراض تطبيق القانون law enforcement purposes" في جميع أقسام قانون الخصوصية.

وأسباب استثناءات تطبيق القانون واضحة: فلسوف تكون معاكسة لتعطى المشتبه فيهم جنائيا والخاضعين للمراقبة القدرة على طلب الملفات التي تخص التحريات الجارية عليهم.

---

(1) Statewatch، US changes the privacy rules to exemption access to personal data cong.press 2007 p 77

(2) Branscomb، Anne، “Who Owns Information?: From Privacy To Public Access”. BasicBooks (1994) p.243

ولذلك، فإن "برامج المطابقة" لا تتضمن مطابقات تم إجراؤها أثناء إجراء عملية تحريات محددة لشخص بعينه.

كما يمكن أيضا لوكالات تطبيق القانون استثناء أنفسها من كثير من متطلبات قانون الخصوصية إذا ما كانت الوظيفة الرئيسة للوكالة تتعلق بتطبيق القوانين الجنائية وإذا كان نظام السجلات يحوي معلومات عن (أ) معلومات حول المذنبين أو المدعى عليهم مثل سجلات إيقافهم أو القبض عليهم وسجلات سابقة الأحكام عليهم، (ب) معلومات تم جمعها لغرض عملية تحريات جنائية مرتبطة بفرد بعينه، أو (ج) تقارير تعريف لفرد تم جمعها أثناء أي مرحلة من مراحل تطبيق القوانين الجنائية من الإيقاف أو القبض على الفرد إلى إيقاف مراقبته.

ومع ذلك، هناك نطاقات محددة في قانون الخصوصية لا يمكن لتطبيق القانون الاستثناء منها. فعلى وكالة تطبيق القانون أن تلتزم بقواعد كشف المعلومات المذكورة بالقسم الفرعي (ب)، بمعنى أنه ليس بإمكانهم كشف معلومات تعريفية شخصية ما لم يكن لديهم موافقة أو أن تكون عملية الكشف عن المعلومات وفق واحدة من الاثني عشر شرطا المذكورة في قسم متطلبات كشف الحكومة عن المعلومات Requirements for Government Disclosure of Information السابق الإشارة إليه.

كما أن على وكالة تطبيق القانون أن تعلن عن وجود وشكل قاعدة بياناتها في السجل الفيدرالي بما في ذلك الاستخدامات اليومية وسياسات تخزين البيانات ومعلومات الاتصال للشخص المسؤول عن النظام. كما يجب على وكالات تطبيق القانون أيضا أن تظل ملتزمة بممارسات تداول المعلومات العادلة بمعنى أن عليها التأكد من دقة واكتمال وميقاتية وترابط السجلات بشكل مناسب، وعليها أن تبذل الجهد المناسب لإبلاغ الفرد متى تم الإفصاح عن سجلاته بناء على أمر من المحكمة أو بناء على مذكرة من المحكمة، كما أن عليها أن تضع قواعد السلوك المناسبة، وضمانات حماية خصوصية المعلومات وتأمينها.

الخامس عشر: الاستخدام الروتيني The routine use[1]

أحد أكثر النصوص المجحفة الشائعة لقانون الخصوصية هي استثناء "الاستخدام الروتيني". أحد الاثني عشر سببا التي قد تتيح لوكالة الإفصاح عن معلومات شخصية هي إذا ما كان الإفصاح هو "للاستخدام الروتيني على نحو ما هو معرف في القسم الفرعي (أ)(7) من هذا القسم، والموصوف في القسم الفرعي (هـ)(4)(د) من هذا القسم".[2]

القسم الفرعي (أ)(7): يعرف "الاستخدام الروتيني" ببساطة على إنه: "استخدام ذلك السجل لأجل غرض يتوافق مع الغرض الذي لأجله تم جمع المعلومات". لاحظ أن الاستخدام الروتيني ليس في حاجة لأن يكون غرضا متطابقا مع الغرض الذي لأجله تم جمع السجل، وإنما غرض متوافق فقط. وغالبا ما يمكن لهذه الصياغة أن تؤدي إلى "التوسع في المهام بما يتعدى الأهداف الأساسية **mission creep**" بالنسبة لنظام السجلات بحيث تتزايد تدريجيا الاستخدامات الروتينية لقاعدة بيانات معينة حتى يتعدى مجالها كثيرا الأهداف المحددة في الأصل.

القسم الفرعي (هـ)(4)(د): يطالب ببساطة أن تكون الاستخدامات الروتينية محددة في السجل الفيدرالي. وفي حين أن ذلك قد يشير إلى ضرورة إدراج جميع الاستخدامات الروتينية المحتملة، فإن الواقع هو أن هذه القوائم غالبا ما تكون متسعة بحيث تشمل كل الاستخدامات المحتملة للبيانات. وفي حين أن بعض قرارات المحاكم قد قيدت المدى الذي تصف به وكالة "الاستخدامات الروتينية".

---

(1) Under the Privacy Act of 1974، the term “routine use” means (with respect to the disclosure of a record) the use of such a record for a purpose that is compatible with the purpose for which it was collected

(2) Law law available at http://foia.state.gov/Learn/PrivacyAct.aspx retrived 12 - 6 - 2013

الفرع الثالث

قانون خصوصية الاتصالات الإلكترونية لسنة 1986

US Privacy of Electronic Communications

Law for the year 1986

قام مجلس النواب الأمريكي بسن قانون خصوصية الاتصالات الإلكترونية لزيادة القيود الحكومية على عمليات التنصت wire taps على المكالمات الهاتفية لتشمل بث أو نقل البيانات الإلكترونية باستخدام الحاسب الآلي (18 U.S.C. §2510 et seq.) حيث أضاف نصوصا جديدة تحظر الدخول على الاتصالات الإلكترونية المخزنة، بمعنى، قانون الاتصالات المخزنة Stored Communications Act (18 U.S.C. §2701 et seq.) وأضاف ما يطلق عليه بأحكام تتبع المكالمات الصادرة والواردة والتي تسمح بتتبع الاتصالات الهاتفية.[1]

ويعد قانون خصوصية الاتصالات الإلكترونية تعديلا للتشريع الثالث Title III للقانون الجامع للتحكم في الجريمة والشوارع الآمنة Omnibus Crime Control & Safe Streets Act لسنة 1968 (قانون التنصت على الهواتف) والذي تم تصميمه أساسا لمنع دخول الحكومة غير المشروع على الاتصالات الإلكترونية الخاصة. ولقد قام قانون دعم الاتصالات في تطبيق القانون Communications Assistance for Law Enforcement Act لسنة 1994، وقانون توحيد وتعزيز

(1) Charles Doyle،Privacy: An Overview of theElectronic Communications Privacy Act، Congressional Research Service،2012 P 10 see also Orin S.$Kerr، THE NEXT GENERATION COMMUNICATIONS PRIVACYACT، Pa. L. Rev،2013

أمريـكا بتوفـير الأدوات المناسـبة واللازمـة لاعـتراض وإعاقـة الإرهـاب Uniting and Strengthening America by Providing Appropriate Tools Required to وقوانـين (Intercept and Obstruct Terrorism (USA PATRIOT) Act (2001 إعـادة ترخيـص وقانـون توحيـد وتعزيـز أمريـكا بتوفـير الأدوات المناسـبة واللازمـة لاعـتراض وإعاقـة الإرهـاب USA PATRIOT reauthorization acts) 2006) وقوانين تعديـلات قانـون مراقبـة الاسـتخبارات الأجنبيـة Foreign Intelligence Surveillance .(Act Amendments Act (2008[1]

و"**الاتصـالات الإلكترونيـة" تعنـي:** أي عمليـة نقـل لعلامـات أو إشـارات أو كتابة أو صـور أو أصـوات أو بيانـات أو معلومـات ذات أي طبيعـة يتـم بثهـا بأكملهـا أو جـزء منهـا بالنظـام السـلكي أو اللاسـلكي أو النظـام الكهرومغناطيـسي electromagnetic أو بالتصويـر الإلكـتروني photoelectronic أو التصويـر البـصري photooptical مـما يكون لـه تأثـير عـلى الولايـات أو التجـارة الخارجيـة إلا أنهـا تسـتثني مـا يلي:

- الاتصالات السـلكية والشفهية.
- الاتصـالات التـي يتم إجراؤها من خلال أجهزة الاسـتدعاء paging device
- الاتصالات مـن أجهزة التتبع tracking device
- معلومـات التحويـلات الماليـة الإلكترونيـة والتـي تقـوم بتخزينهـا المؤسسـات الماليـة في نظـام الاتصـالات المسـتخدم للتخزيـن الإلكـتروني وتحويـل الأمـوال.

---

(1) Brendan Sasso، Consensus Builds for Requiring Warrant for Email(The Hill Searches،) 2013 P 27، March$ 19،$ 2013،$

ويحمي التشريع الأول Title I لقانون خصوصية الاتصالات الإلكترونية الاتصالات السلكية والشفهية والإلكترونية وهي تبث. ويحدد التشريع متطلبات مذكرات warrants البحث والتي تعد أكثر صرامة من أي بيئة setting أخرى. ويحمي التشريع الثاني لقانون خصوصية الاتصالات الإلكترونية - قانون الاتصالات المخزنة Stored Communications Act الاتصالات المحتفظ بها إليكترونيا وأبرزها الرسائل المخزنة على الحاسبات الآلية.

ومع ذلك، نجد أن سبل حمايتها تعد أضعف مما يرد في التشريع الأول، ولا تفرض معايير عالية على المذكرات. ويمنع التشريع الثالث استخدام أجهزة تتبع المكالمات الصادرة والواردة لتسجيل معلومات الاتصال والتحويل والموجهة والإشارة والمستخدمة في عملية بث الاتصالات السلكية والإلكترونية دون الحصول على أمر من المحكمة.[1]

و قد زاد قانون خصوصية الاتصالات الإلكترونية من القيود على عمليات التنصت على المكالمات الهاتفية ليشمل عمليات بث البيانات الإلكترونية عبر الحاسبات الآلية وأضاف أحكاما جديدة تمنع الدخول على الاتصالات الإلكترونية المخزنة أي قانون الاتصالات المخزنة وأضافت أحكام المكالمات الصادرة والواردة والتي تسمح بتتبع الاتصالات الهاتفية.[2]

ووفقا للتشريع 18 يجوز للوكالات الفيدرالية أن تستدعي الرسائل الإلكترونية التي يتعدى تاريخها 180 يوما.

---

(1) Helft، Miguel and Claire Cain Miller، "News Analysis: Privacy Law Is Outrun by the Web"، (1986) p.25

(2) Brendan Sasso and Jennifer Martinez House to Consider Email Privacy Bill، The Hill، 2013،$ available at http://thehill.com/blogs/hillicon`valley/technology/285397`overnight`tech`house`to`consider`email`privacy`bill$

ويتيح التشريع أوامر قضائية أو حكومية تحظر نشر المعلومات أو التعليقات علانية وفي بعض الحالات نقلها إلى طرف ثالث غير مرخص له gag orders والتي توجه المتلقي لأمر التشريع بالامتناع عن كشف وجود الأمر أو التحريات.

كما يتيح التشريع أوامر قضائية أو حكومية تحظر نشر المعلومات أو التعليقات علانية وفي بعض الحالات نقلها إلى طرف ثالث غير مرخص له والذي يوجه المتلقي لأمر تسجيل المكالمات الصادرة والواردة بعدم كشف المكالمات الصادرة والواردة أو التحريات.[1]

أثارت عدة قضايا رفعت بالمحاكم سؤالا حول ما إذا كان يتم حماية الرسائل الإلكترونية وفقا للأحكام الصارمة للتشريع الأول في الوقت التي تكون فيه هذه الرسائل مخزنة تمهيدا للإرسال إلى متلقيها النهائي.

في قضية الولايات المتحدة ضد كاونسيلمان United States v. Councilman حكمت محكمة مقاطعة أمريكية ومنصة قضاء من ثلاثة قضاة بعدم جواز ذلك إلا أنه في عام 2005، نقضت محكمة الاستئناف الأمريكية للدائرة الأولى هذا الرأي. فقد تم تأييد مناصري الخصوصية حيث أبدوا في مذكرة أصدقاء المحكمة Amicus curiae أنه إذا كان قانون خصوصية الاتصالات الإلكترونية لم يقم بحماية الرسائل الإلكترونية تحت الإرسال، فإن سبل الحماية الإضافية التي يسرتها لم يكن لها معنى حيث إننا في الواقع نجد أن كل الرسائل الإلكترونية يتم تخزينها مؤقتا قبل الإرسال مرة واحدة على الأقل، كما أن مجلس الشيوخ كان عليه أن يعرف ذلك في عام 1986 عندما تم تمرير القانون. ولقد تم رفض القضية في النهاية على أساس عدم ارتباطها بقضايا قانون خصوصية الاتصالات الإلكترونية.[2]

---

(1) "Office of Justice Programs (OJP)، U.S. Department of Justice (DOJ)". Retrieved 2013. P.24

(2) John،. A.،A Application of the United States of America privacy laws of January 25، 2013 p.37

ووفقا لقانون التنصت اللاسلكي الفيدرالي، والمعدل بالتشريع الأول لقانون خصوصية الاتصالات الإلكترونية، فإن التحفظ على حاسب آلي مستخدم في تشغيل نظام نشرات إليكترونية ويحوي رسائل إليكترونية خاصة تم إرسالها إلى (مخزنة في) لوحة النشرات ولكن لم يقم بقراءتها المتلقين المرتقبين لا يشكل اعتراضا غير قانوني.

فبإمكان الحكومات في واقع الأمر تتبع المكالمات الهاتفية في وقتها دون الحصول على أمر تفتيش وفقا لقانون خصوصية الاتصالات الإلكترونية من خلال تحليل المعلومات من خلال الهوائي المتصل بالهواتف الخلوية طالما أن الهاتف الخلوي يستخدم علانية وحيثما تتوافر المراقبة البصرية.

في قضية روبنيز ضد مقاطعة مدرسة لور ميريون Robbins v. Lower Marion School District (2010) والمعروفة ببوابة كاميرا الويب WebcamGate، اتهم المدعون قيام مدرستين ثانويتين في ضواحي فيلادلفيا بانتهاك قانون خصوصية الاتصالات الإلكترونية بالتشغيل عن بعد كاميرات الويب المثبتة في اللاب توب الذي تسلمه المدرسة للطلاب وقاموا بمراقبة الطلاب في المنازل. واعترفت المدرسة بأنها تقوم سرا بأخذ لقطات لما يزيد عن 66 ألف لقطة عن طريق كاميرا الويب للطلاب في غرف نومهم.[1]

تم انتقاد قانون خصوصية الاتصالات الإلكترونية لفشله في حماية جميع الاتصالات وتسجيلات المستهلكين وذلك أساسا لأن القانون عفى عليه الزمان وليس على دراية بالكيفية التي يقوم بها الأفراد اليوم بتبادل وتخزين

---

(1) Doug Stanglin "School district accused of spying on kids via laptop webcams". USA Today. 2010. Article See also Sasso & Martinez، (reporting the commitment of House Judiciary Chairman Robert Goodlatte to "look at modernizing the decades'old Electronic Communications Privacy Act (ECPA)$ to$ reflect$ our$ current$ digital$ economy"). supra note، 2013

واستخدام المعلومات. فعلى سبيل المثال، وفقا لقانون خصوصية الاتصالات الإلكترونية، من اليسير نسبيا على وكالة حكومية أن تطالب بأن يسلم مقدمي الخدمة بيانات العملاء الشخصية والتي تم تخزينها في خوادمها servers.

فعلى سبيل المثال، البريد الإلكتروني المخزن لدى خادم طرف ثالث لما يزيد عن 180 يوما يعد مهملا من قبل القانون وإن كل ما يلزم لحصول وكالة لتطبيق القانون على محتوى البريد الإلكتروني هو إفادة خطية تقر بأن المعلومات معنية بأحد التحريات ودون الحاجة إلى مراجعة قضائية.

عندما تم تمرير القانون في البداية، كانت الرسائل الإلكترونية يتم تخزينها في خادم طرف ثالث لفترة قصيرة من الوقت وهي فترة طويلة بالقدر الذي ييسر نقل الرسالة الإلكترونية إلى البريد الإلكتروني للعميل والذي كان بشكل عام موجود على حاسبه الشخصي أو الحاسب الآلي بالعمل.

والآن، مع خدمات البريد الإلكتروني الشائعة مثل Hotmail وGmail، الأكثر احتمالا أن يخزن المستخدمون البريد الإلكتروني على النت لفترة غير محددة عن الاحتفاظ به لمدة تقل عن 180 يوما.

فإذا ما تم تخزين البريد الإلكتروني نفسه على الحاسب الآلي للمستخدم، فلسوف يلزم الشرطة الحصول على مذكرة للحصول على محتوياتها بغض النظر عن عمر البريد الإلكتروني. وعندما يتم تخزينها على خادم الإنترنت، فلن تكون هناك حاجة إلى مذكرة بدءا من 180 يوما بعد استلام الرسالة وفقا للقانون. وفي عام 2013، اقترح أعضاء مجلس النواب الأمريكي إصلاح هذا الإجراء.

ولقد زاد قانون خصوصية الاتصالات الإلكترونية أيضا من قائمة الجرائم والتي تبرر استخدام المراقبة إلى جانب عدد من القانونيين الذين يمكنهم التصريح بإجراء مثل هذه المراقبات.

فبيانات الأفراد أو المجموعة يمكن الحصول عليها أثناء انتقالها أو

بأساليب استدعاء، ودون الحاجة إلى مذكرة تفتيش warrant، مما يسمح لوكالة بالحصول على معلومات استخبارتية قيمة وربما غزو الخصوصية دون أي تدقيق ذلك لأنه لا يتم المساس بالمحتوى الحقيقي للاتصالات.

وفي حين أن الاتصالات في أماكن العمل تعد مؤمنة من الناحية النظرية، فإن كل ما يلزم للدخول على بيان رسمي هو ببساطة بالنسبة لصاحب العمل بإعطاء إشعار أو أن يشعر المشرف أن أفعال الموظفين ليست في مصلحة الشركة. وهو ما يعني أنه مع أدنى الافتراضات، يمكن لصاحب العمل أن يراقب الاتصالات داخل الشركة.

والجدال الدائر في متى يتم تقييد سلطة الحكومة في التدخل في حياة المدنيين في حين أن موازنة الاحتياج لتطويق التهديدات المحلية.[1]

في عام 2011، نشرت النيويورك تايمز "قانون الخصوصية لسنة 1986 يتم تجاوزه بالشبكة العنكبوتية" مركزين على أن:

في الأعوام الماضية جادلت وزارة العدل في المحاكم على أن مستخدمي الهواتف الخلوية قد تخلوا عن توقعهم الخصوصية بشأن موقعهم بإعطاء تلك المعلومات إلى الشركات الناقلة اختياريا. وفي أبريل، جادلت في محكمة فيدرالية في كولورادو بأن عليها الدخول على بعض البريد الإلكتروني دون الحاجة إلى مذكرة تفتيش. ويخطط مسؤولو تطبيق القانون الفيدراليون بالاستشهاد بعمليات التقدم التكنولوجي للمطالبة بلوائح جديدة تساعد على تيسير قدرتهم على تنفيذ عمليات التنصت القانونية لمختلف الاتصالات الواردة على الإنترنت.

واستمر التحليل ليناقش كيف أن "جوجل" و"فيس بوك" و"فريزون" و"تويتر" وغيرها من الشركات في الوسط بين المستخدمين والحكومات.[2]

---

(1) Electronic Communications Privacy Act of 1986 (ECPA)، retrived 2013 p.25 https://it.ojp.gov/default.aspx?areaprivacy&page1285

(2) Andrea Peterson، "Privacy Protections for Cloud E - mail"، Think Progress، (March 20، 2013) p.63.

ونخلص من ذلك إلى أن هذا القانون لم يعد يتماشى مع التطور التكنولوجي حيث إنه يسمح بالحصول على المعلومات أثناء انتقالها، الأمر الذي أصبح في غاية السهولة إثر التطور التقني ومن ثم لم يعد يفرض القانون الحماية المطلوبة والمرجوة منه، إضافة إلى أنه لا يفرض أية حماية قانونية على الشركات الناقلة للبيانات والشركات المضيفة للخدمة مما يؤدي إلى انتهاك خصوصية الأفراد بشكل مستمر الأمر الذي نظمه قانون حماية خصوصية المستهلك لعام 1997.

الفرع الرابع

قانون حماية خصوصية المستهلك لعام [1]1997

إن هذا القانون هو الذي ينظم كيف يمكن لشركات تقديم خدمات البرامج التفاعلية (هي شركات تقديم خدمات المعلومات أو الدخول على المعلومات لمجموعة متعددة من المستخدمين) أن يستخدم مدخلات المستخدمين لبياناتهم الشخصية.

ولأغراض مشروع القانون هذا، فإن شركات تقديم خدمات البرامج التفاعلية تتمثل في الأساس في مقدمي خدمة الإنترنت.

ويحظر قانون حماية خصوصية المستهلك لسنة 1997 على شركات تقديم خدمات البرامج التفاعلية أن تكشف لطرف ثالث عن أي معلومات تعريفية شخصية قدمها المشترك دون الموافقة المكتوبة للمشترك بالعلم. كما يسمح للمشترك بإبطال مثل هذه الموافقة في أي وقت ويطالب شركة تقديم الخدمة عن التوقف عن كشف مثل هذه المعلومات.[2]

ويحظر القانون شركات تقديم الخدمة أو موظفيها من الكشف عن قصد إلى طرف ثالث أي معلومات تعريفية شخصية يقدمها المشترك مما تكون شركة الخدمة قد زيفتها أو شوهتها.

يطالب القانون وبناء على طلب المشترك أن تقوم الخدمة ب (1) تزويد

---

(1) Angela Choy،Marcia S.Smith and Jane Bortnick Griffith، Protecting privacy on the internet: a summary of legislative proposal،"CRS Report for Congress،Congressional Reasearch Service،The liberary of Congress" (1997) p.135

(2) Lanier and Saini/Understanding Consumer Privacy: A Review and Future Directions و Academy of Marketing Science.2008 ؛ p 24

مثل هـذا الفـرد بمعلوماتـه التعريفيـة الشـخصية التي تحتفـظ بها شركة تقديـم الخدمة، (2) بالسـماح للمشـترك بالتحقـق مـن مثـل هـذه المعلومـات وتصحيحهـا، (3) تعريـف المشـترك بمتلقـي المعلومـات لطـرف ثالث.

يحظـر عـلى شركـة تقديـم الخدمـة مـن فرض رسـم على المشـترك نظير إتاحـة مثل هـذه المعلومات.

يمنـح القانـون مفوضيـة التجـارة الفيدراليـة السـلطة ل (1) تحـري مـا إذا كانـت شركـة تقديـم الخدمـة متورطـة أو مشـاركة في أي عمـل أو ممارسـة يحظرهـا هـذا القانـون، و(2) إذا كان الأمـر كذلـك، إصـدار أمـر إيقـاف ومنـع كـما لـو كانـت شركـة تقديـم الخدمـة تنتهـك أحكامـا محـددة مـن قانـون مفوضيـة التجـارة الفيدراليـة.[1]

يسـمح القانـون للمشـترك المتضرر مـن انتهـاك هـذا القانـون الحصـول عـلى التعويـض المناسـب مـن خـلال الدعـاوى المدنيـة.

لتنظيـم اسـتخدام شركات تقديـم خدمـات البرامـج التفاعليـة لمعلومـات التعريف الشـخصية التـي يزود المشـتركين بهـا شركات تقديـم الخدمة.

و قـد وضع القانـون تعريفات محـدده للمصطلحات حيث أوضح أن:

1. تعبـير "شركـة تقديـم خدمـة البرامـج التفاعليـة interactive computer service" قـد تعنـي شركـة خدمـة المعلومـات التـي تتيـح دخـول عـدد مـن مسـتخدمي الحاسـب الآلي عـلى الإنترنـت عـبر مـودم.
2. تعبـــير "إنترنـــت Internet" يعنـــي شـــبكة الحاســـبات الدوليـــة لـــكل

(1) John Villasenor، Recording Everything Digital Storage as an Enabler of Authoritarian Governments، Brookings Institution، available at http://www.brookings.edu/~/media/research/files/papers/201120%14/12/digital P25

مـن لشـبكات البيانـات القابلـة للتشـغيل المتبـادل الفيدراليـة وغـير الفيدراليـة.

3. تعبـير "المعلومـات التعريفيـة الشـخصية personally identifiable information" تحمـل المعنـى الموضـح لهـذا التعبـير في القسـم رقـم 631 مـن قانـون الاتصـالات لسـنة 1934 (47 U.S.C. 551)

4. تعبـير "الموافقـة الكتابيـة بالعلـم informed written consent" يعنـي إقـرار:

أ. مكتـوب وموقع بحرية من قبل المشـترك.

ب. بالموافقـة عـلى عمليـات الكشـف والإفصـاح عـن المعلومـات التـي سـتتيحها شركـة تقديـم الخدمـة.

ج. بوصف حقوق المشـترك وفقـا لهذا القانون.

5. تعـبر "الطـرف الثالـث third party" يعنـي فيـما يتعلـق بالكشـف عـن المعلومـات التعريفيـة الشـخصية التـي يقدمهـا المشـترك لشركـة تقديـم خدمـات البرامـج التفاعليـة، شـخص أو أي كيـان أخـر عـدا:

أ. مقـدم هذه الخدمة.

ب. موظف بشركـة تقديم الخدمة.

ج. المشـترك في هذه الخدمة.

وحيـث إن هـذا القانـون قـد سـنه نـواب مجلـس الشـيوخ والنـواب في الولايـات المتحـدة في اجتـماع المجلـس، فإنـه يمكـن وصـف هـذا القانـون "بقانون حمايـة خصوصية المسـتهلك عـلى الإنترنت".

وفي قانـون سـنة 1997 وكذلـك لائحـة تنظيـم اسـتخدام شركات تقديـم الخدمـات للمعلومـات التعريفيـة الشـخصية للمشـترك نجـد التـالي: [1]

أ. يحظـر الكشـف عن المعلومـات التعريفية الشـخصية دون تأمين الموافقة.

1. بشـكل عـام، لـن تكشـف شركـة تقديـم خدمـة الحاسـب الآلي التفاعـلي أي معلومـات تعريفيـة شـخصية إلى طـرف ثالـث يقـوم المشـترك بتزويدهـا دون الموافقـة المكتوبـة المسـبقة للمشـترك.

2. إلغـاء الموافقـة - ستسـمح شركـة تقديـم الخدمـة للمشـترك بإلغـاء الموافقـة الممنوحـة في الفقـرة (1) في أي وقـت وبنـاء عـلى هـذا الإلغـاء، سـتقوم شركـة تقديـم الخدمـة بكشـف هـذه المعلومـات إلى طـرف ثالـث.

ب. يحظـر الكشـف عـن معلومـات تعريفيـة شـخصية مزيفـة – لـن تقـوم شركـة تقديـم الخدمـة أو أي موظـف بهـا بالكشـف المتعمـد لطـرف ثالـث عـن أي معلومـات تعريفيـة شـخصية يقدمهـا المشـترك تعلـم أنهـا مزيفـة.

ج. دخول المشـترك على معلومات التعريف الشـخصية:

1. بشـكل عـام، بنـاء عـلى طلـب المشـترك، سـوف تقـوم شركـة تقديـم خدمـة البرامـج التفاعليـة:

أ. تقديـم البيانـات التعريفيـة الشـخصية التـي تحتفـظ بهـا شركـة تقديـم الخدمة إلى المشترك.

(1) Orris & Truskowsi noting that since 1997 raw،storage،prices have been declining، supra note 1998 P 56 See also Peter Swire، From RealH Time Intercepts to Stored Records: Why،Encryption Drives the Government to Seek Access to the Cloud، available at.http://papers.ssrn.com/sol3/papers.cfm?abstract_id2038871.$ 2001 P12

ب. تسـمح للمشـترك بالتحقـق مـن المعلومـات التـي تحتفـظ بهـا شركـة تقديـم الخدمـة.

ج. تسـمح للمشـترك بتصحيح أي خطأ في هذه المعلومات.

2. الدخـول عـلى شـخصية المتلقـين للمعلومـات - بنـاء عـلى طلـب المشـترك، تقـوم شركـة تقديـم الخدمـة بتحديـد شـخصية الطـرف الثالـث المتلقـي للمعلومـات التعريفيـة الشـخصية للمشـترك.

3. الرسـم - بنـاء عـلى هـذا القسـم الفرعـي، لـن تقـوم شركـة تقديـم الخدمـة بفـرض رسـم عـلى المشـترك نظـير توفـير المعلومـات.

وفي القسـم الثالـث والخـاص بالتطبيق والإعفاء فإن: [1]

أ. مفوضيـة التجـارة الفيدراليـة - سـوف يكـون لدى مفوضيـة التجـارة الفيدرالية السـلطة للتفتيـش عـلى شركات تقديـم خدمـات البرامـج التفاعليـة والتحـري عنهـا للتأكـد عـما إذا كانـت هذه الشركـة متورطة أو مشـتركة في أي عمـل أو ممارسـة محظـورة وفقـا لهـذا القانـون.

ب. الإعفاء.

1. أمـر الإيقـاف والإبطـال - إذا ما قررت مفوضيـة التجـارة الفيدرالية بأن إحدى شركات تقديـم خدمـات البرامـج التفاعليـة متورطـة أو مشـاركة في أي عمل أو ممارسـة محظـورة وفقـا لهـذا القانـون، يجـوز للمفوضية أن تصدر أمـر إيقاف وإبطـال إذا مـا ثبـت انتهـاك شركـة تقديم الخدمة للقسـم الخامـس من قانون مفوضيـة التجـارة الفيدرالية.

2. الدعـوى المدنيـة - يجـوز للمشـترك المتـضرر مـن انتهـاك القسـم الثـاني الحصـول عـلى التعويـض المناسـب بالدعـوى المدنيـة.

(1) Consumer Privacy act report "Office of Justice Programs (OJP)، U.S. Department of Justice (DOJ)". Retrieved 2013. P 86

نخلص مما سبق أن قانون حماية المستهلك لعام 1997 قد حصن المستهلك ضد انتهاكات الشركات التي تقدم خدمة الإنترنت من حيث الإفصاح عن البيانات المسجلة لدى الشركات المضيفة بأنه قرر عقوبات على إفشاء تلك البيانات حتى وإن كانت بيانات مغلوطة ووفر القانون الحماية القانونية للبيانات والمعلومات وحق المستهلك في الحصول على التعويض الملائم لتضرره من إفشاء مثل هذه المعلومات.

بالإضافة إلى ذلك فإنه وضع تعريفات واضحة لكل من الشركات مقدمة الخدمة والطرف الثالث وكذلك معلومات التعريف الشخصي ومفهوم الإنترنت مما أدى إلى سهولة ضبط الشركات التي تفشي البيانات وتجديد الفعل الضار التي تقوم به.

الفرع الخامس

قانون حماية خصوصية الضمان الاجتماعي على الخط لعام 1997

Social Security On - line Privacy Protection Act of 1997[1]

صدر لتنظيم استخدام شركات تقديم خدمات البرامج التفاعلية لأرقام الضمان الاجتماعي ومعلومات التعريف الشخصية الآخر في عام 1997.

وقد قام بسن هذا القانون نواب مجلسي الشيوخ والنواب الأمريكي.

يجوز التنويه إلى هذا القانون ب"قانون حماية خصوصية بيانات الضمان الاجتماعي على شبكة الإنترنت لسنة 1997.

ويحظر نشر رقم حساب الضمان الاجتماعي أو معلومات التعريف الشخصية المرتبطة به دون الحصول على موافقة – لا يحق لشركة تقديم خدمة البرامج التفاعلية من خلال خدمة مرجعية أو غير ذلك أن تكشف لطرف ثالث:

1. رقم حساب الضمان الاجتماعي للفرد.
2. معلومات تعريفية شخصية والتي تعرف شخص من خلال رقم حساب الضمان الاجتماعي للفرد بدون الحصول على الموافقة الكتابية المسبقة بالعلم.

ويجوز إلغاء الموافقة – تسمح شركة الخدمة للفرد بإلغاء أي موافقة ممنوحة وفقا للفقرة السابقة في أي وقت، ولسوف تتوقف شركة الخدمة عن كشف مثل هذا الرقم أو المعلومات لطرف ثالث.

---

(1) Privacy & Disclosure Law and Guidance، http://www.ssa.gov/foia/html/disclosure_law.htm retrived at 22 - 12 - 2013 p.11

كما أن مفوضية التجارة الفيدرالية - تخول مفوضية التجارة الفيدرالية للتفتيش على شركات تقديم خدمة البرامج التفاعلية والتحري عنها لتحديد ما إذا كانت شركة الخدمة متورطة أو مشاركة في أي عمل أو ممارسة يحظرها هذا القانون.

إذا قررت مفوضية التجارة الفيدرالية أن شركة تقديم خدمة البرامج التفاعلية متورطة أو مشاركة في أي عمل أو ممارسة يحظرها هذا القانون، يجوز للمفوضية أن تصدر أمر إيقاف كما لو أن شركة تقديم الخدمة هذه تنتهك القسم الخامس من قانون مفوضية التجارة الفيدرالية وأن تكون مسؤولة عن عمليات انتهاك مثل هذا الأمر على نحو ما هو مبين في القسم الخامس. كما أن أي شركة تقديم خدمات مشاركة في عمل أو ممارسة يحظرها هذا القانون عن علم أو ضمنا على أساس ظروف موضوعية أن هذا العمل أو الممارسة محظورة سوف تكون عرضة لعقوبات مدنية وفقا للقسم رقم 5 (م)(1) من هذا القانون إذا ما كانت شركة الخدمة تلك تنتهك القسم الخامس.[1]

و بالنسبة للتعريفات المهمة التي أوردها هذا القانون فهي كالأتي[2]:

1. تعبير"شركة تقديم خدمة البرامج التفاعلية interactive computer service" يعني أي خدمة المعلومات التي تتيح دخول عدد من مستخدمي الحاسب الآلي على الإنترنت عبر مودم وسائل اتصالات أخرى للإنترنت أو أي شبكات عاملة على الإنترنت.
2. تعبير "إنترنت Internet" يعني شبكة الحاسبات الدولية لكل

(1) Angela Choey،Protecting Privacy on the internet: Alegislative Proposal 1997 P 7

(2) John C. Yates،Privacy & Data - Mining On The Internet،1999 P2 available at http://www.mmmlaw.com/media - room/publications/articles/privacy - data - mining - on - the - internet

مـن لشـبكات البيانـات القابلـة للتشـغيل المتبـادل الفيدراليـة وغـير الفيدراليـة.

3. رقـم حسـاب الضـمان الاجتماعـي Social Security Account Number - يعنـي رقـم حسـاب الضـمان الاجتماعـي للفـرد هـو الرقـم المخصـص لهـذا الفرد

4. تعبـير "المعلومـات التعريفيـة الشـخصية personally identifiable information" تحمـل المعنـى الموضـح لهـذا التعبـير في القسـم رقـم 631 مـن قانـون الاتصـالات لسـنة 1934.

5. الموافقـة المعلومـة بالعلـم Informed Written Consent الموافقة المكتوبة بالعلـم للفـرد تعنـي بيـان:

أ. مكتـوب ويوقعهـا الفرد بحرية.

ب. بالموافقـة عـلى كشـف شركات تقديـم الخدمـة هـذه للمعلومـات التـي يتـم تزويدهـا بهـا.

ج. يصـف حقوق الفرد وفقـا لهذا القانون.

6. الطـرف الثالـث Third Party - ويعنـي الطـرف الثالـث فيـما يتعلـق بعملية كشـف رقـم حسـاب الضـمان الاجتماعـي أو أي معلومـات تعريفيـة شـخصية مرتبطـة بهـذا الفـرد، أي شـخص أو كيـان غـير:

أ. شركـة تقديم الخدمة.

ب. أحـد العاملين بشركـة تقديم الخدمة.

ج. الفرد.

و يـري الباحـث أن هـذا القانـون قـد أضـاف حمايـة لبيانـات التعريـف الشـخصي للفـرد، وخاصـة رقـم الضـمان الاجتماعـي، كـما أنـه أضـاف ذلـك ضمـن

التعريفـات المهمـة للقانـون، وكذلـك أوضـح القانـون مفهـوم شركـة تقديـم خدمـة البرامـج التفاعليـة بوضـوح ولم يقتـصر كسـابقه عـلى فكـرة الـشركات مقدمـة الخدمـة أو المضيفـة.

كـما أنـه منـح الحريـة للفـرد في إلغـاء الموافقـة الممنوحـة للشركات مقدمـة الخدمـة في الكشـف عـن بيانـات التعريـف الشـخصي ورقـم الضـمان الاجتماعـي الخـاص بـه، وقـد فـرض هـذا القانـون اهتماماً خاصـا برقـم الضـمان الاجتماعـي حيـث إنـه مـن خـلال هـذا الرقـم يسـهل الوصـول إلى بيانـات التعريـف الشـخصي للفـرد.

الفرع السادس

قانون خصوصية الاتصالات لعام 1997.

Encrypt Communications Privacy Act of 1997[1]

يسمح قانون خصوصية الاتصالات المشفرة لسنة 1997 لأي فرد داخل أي ولاية وأي فرد أمريكي يعيش في دولة أجنبية باستخدام أي تشفير، وبغض النظر عن لوغارتمية التشفير المستخدمة، أو الطول الرئيس المختار key length chosen أو أسلوب التنفيذ أو الوسيط المستخدم مع الاستثناءات. ويحظر القانون على الحكومة الفيدرالية أو الولاية من المطالبة كشرط تسويقي أن يتم منح مفتاح التشفير إلى شخص أخر.[2]

يحدد القانون بأنه لا يوجد بالقانون ما يتم تفسيره على أنه: (1) يتطلب استخدام أي شكل من أشكال التشفير، أو (2) يحد من التأثير على قدرة أي شخص على استخدام التشفير دون ضمان استخدام الترتيبات المعنية بالمفاتيح اللازمة لفك شفرة البيانات المشفرة key escrow function، أو أي شخص يختار استخدام تشفير بوظيفة ضمان رئيسة غير مستخدمة إلا أن يستخدم مفتاح رئيس key holder.[3]

يقوم قانون خصوصية الاتصالات المشفرة بتعديل القانون الجنائي الفيدرالي ليخضع للعقوبات الجنائية والمسؤولية المدنية أي حامل لمفاتيح

(1) Encrypt Communications Privacy Act of 1997http://thomas.loc.gov/cgi - bin/query/z?c105:S.376 retrived 122013/5/

(2) Encryption: Impact on Law Enforcement،، "seal omitted Facility Quantico، Virginia"، (1998) p. 22

(3) CHarisse Castagnoli، Someone›s Been Reading My E - Mail! Privacy Protection for Electronic Mail Users in the US and EC، 9 COMPUTER، L. & PRAC.،، (1993).p 6

التشفير يقوم بدون ترخيص بتزويد مفاتيح التشفير أن من يقدم المساعدة على فك التشفير.

كما أن قانون خصوصية الاتصالات المشفرة يجعل الدفاع متكاملا ضد أي من الأفعال المدنية أو الجنائية التي يؤتيها المدعى عليه استنادا إلى أمر من المحكمة، أو استدعاء من هيئة المحلفين الكبرى أو المحكمة أو لترخيص قانوني. ويصرح القانون لحامل مفاتيح التشفير الكشف عن مفتاح فك التشفير أو تقديم المساعدة على فك التشفير لكيان حكومي يحتاج إلى الكشف عن اتصالات مخزنة سلكية أو إلكترونية والكشف عن سجلات المعاملات المالية، إلى جانب المعلومات المخزنة طالما تم تلبية متطلبات أمر المحكمة المناسب.[1]

ويوجه القانون النائب العام وغيره من المسؤولين المحددين إلى إبلاغ المكتب الإداري للمحاكم الأمريكية بعدد الأوامر أو التمديدات التي تم طلبها بشأن مفاتيح فك التشفير لأجل الحصول على مدخل لمفاتيح فك التشفير أو لطلب المساعدة في فك التشفير.[2]

ويحدد القانون العقوبات للمحاولات المتعمدة من خلال عمليات التشفير لإعاقة أو عرقلة أو منع الاتصالات التي يجريها مسؤول معلومات عن تحريات أو لتطبيق القانون بشأن جناية.[3]

كما يسمح القانون لأي فرد داخل أي الولاية ببيع أي تشفير من خلال تجارة بين الولايات. ويمنح وزير التجارة السلطة الحصرية لرقابة صادرات

---

(1) Mark L. Goldstein and Lisa S. Vogel، Can You Read Your Employees› E - mail?" N.Y.L.J.، 1997، p 1

(2) Paul E. Hash and Christina M. Ibrahim، E - Mail، Electronic Monitoring، and Employee Privacy، 37 SOUTH TEXAS LAW REVIEW 893 (1996). P 3

(3) Elsa F. Kramer، The Ethics of E - Mail، RES GESTAE، Jan. 1996، p 24.

كافة أجهزة وبرامج وتكنولوجيا الحاسبات الآلية والتي يتم تصميمها أو تعديلها خصيصا لأجل الاستخدام العسكري.(1)

يحظر القانون الحصول على أي رخصة سارية (مع وجود استثناءات محدودة) لتصدير أو إعادة تصدير أي من:

1. البرامج بما في ذلك البرامج ذات قدرات التشفير والمتوافرة بشكل عام على ما هي عليه ومصممة ليقوم المشتري بتركيبها، أو التي في النطاق العام domain أو المتاحة للجمهور نظرا لكونها متاحة بشكل عام لدخول الجمهور عليها بأي شكل من الأشكال.

2. أجهزة الحاسب فقط لأنها تتضمن أو تشغل بأي شكل برامج (بما في ذلك برامج ذات قدرات تشفيرية) مستثناة من أي من المتطلبات اللازمة لرخصة صالحة.

3. البرامج أو الأجهزة غير المحظورة ذلك لأنها تتضمن آليات وسطية للتفاعل مع البرامج والأجهزة الأخرى.

4. تكنولوجيا التشفير المرتبطة بالأجهزة أو البرامج أو المعدات الموصوفة في البنود من (1) إلى (3).

يوجه القانون الوزير للترخيص بتصدير أو إعادة تصدير البرامج أو الأجهزة أو التكنولوجيا ذات قدرات التشفير دون استثناء الحصول على ترخيص إذا:

1. كان هناك منتج يعرض برنامج تأمين مقارن متاح تجاريا من موزع أجنبي دون قيود فعالة.

---

(1) Note، Keeping Secrets in Cyberspace: Estabishing Fourth Amendment Protection for Internet Communication، 110 HARV. L. REV. 1591 (1997).

2. كان هنـاك منتـج مقارن متاح بوجه عـام في دولة أجنبية.

3. الأسـاس الوحيـد لمنـع اسـتثناء الرخصـة يكمـن في تطبيـق تشـفير مـن مصـدر أجنبـي.[1]

يوجـه القانـون الوزيـر إلى حظـر تصدير أو إعـادة تصدير أي مـن برامج ومعدات وتكنولوجيـا الحاسـب الآلي إلى دولـة أجنبيـة إذا مـا قـرر الوزيـر أن هنـاك دليلا مادي أن مثـل هذه المعـدات أو التكنولوجيا سـوف:

1. تتحول إلى الاسـتخدام العسـكري أو تسـتخدم في دعم الإرهاب الدولي.

2. يتـم تعديلها لمثل تلك الاسـتخدامات.

3. يعـاد تصديرهـا بدون الحصول على ترخيص مـن الولايات المتحدة.[2]

يحظـر القانـون عـلى أي مسـؤول عـن التحريـات أو تطبيـق القانـون أو المسـؤول عـن مفاتيـح التشـفير مـن الكشـف عـلى مفاتيـح فـك التشـفير أو تقديـم المسـاعدة في عمليـة فـك التشـفير إلى دولـة أجنبيـة باسـتثناء عندمـا تدخـل الولايـات المتحـدة في معاهـدة أو اتفاقيـة مـع دولـة أجنبيـة لتقديـم المسـاعدة المتبادلـة في عمليـات فـك التشـفير. يعلـن القانـون أنـه لا يوجـد في هـذا القانـون:

1. ما يشـكل السلطة لإجراء أنشطة اسـتخباراتية.

2. مـا يؤثـر عـلى الطريقـة المحـددة التـي يتبعهـا المسـؤولين أو العاملـين الفيدراليـين فيـما يخـص تأمـين الاتصـالات والاتصـالات التـي تجريهـا القـوى الأجنبيـة أو العمـلاء فيـما بينهـم.[3]

---

(1) Michael J. Patrick، E - Mail Data Is a Ticking Time Bomb، NAT›L L.J.، Dec. 20، 1993، p 13.

(2) Kenneth R. Shear، What You Don›t Know Can Hurt You: E - Mail Privacy Claims Under the Federal Electronic Communications Privacy Act، LAW OFF. ECON. & MGMT. (1996). P 49

(3) Mark K. Smallhouse، Drafting Effective E - Mail Policies، PREVENTIVE L. REP. (1995).p 4

نخلص مما سبق إلى أن هذا القانون الذي يتعامل مع تشفير البيانات ثم بعد ذلك دخول نطاق البرامج هو من القوانين التي تفرض حماية ذات بعد مختلف للخصوصية إلى جانب أن القانون لم يعط الحق في فك التشفير إلا بحكم من المحكمة والحالات التي تهدد الأمن القومي.

و الجدير بالذكر أن التشفير وخاصة للبرامج خروجا من دائرة البيانات الشخصية يعد أمراً حتمياً، حيث إن العصر الرقمي الذي نواكبه منح القدرة على التعدي على حقوق الغير فمثل هذه البرامج تعد أموالا واستثمارات ومن ثم وجب فرض تلك الحماية القصوى عليها، وعلى ذلك يكون التشفير هو الوسيلة المثلى لمثل هذه الحماية.

الفرع السابع

قانون الخصوصية الشخصية على الإنترنت لسنة 2001 و2002

Online Personal Privacy Act[1]

حماية الخصوصية على الإنترنت - يحظر القانون مقدم خدمة الإنترنت أو مقدم الخدمات باستخدام الإنترنت أو (مقدم) أو مشغل المواقع التجارية من جمع أو كشف المعلومات التعريفية الشخصية (الاسم - العنوان - رقم الهاتف) للمستخدم دون إشعار واضح وجلي للمستخدم. ويطالب القانون مقدم الخدمة أن:

1. يحصل على موافقة مكتوبة أو إلكترونية مؤكدة لجمع وكشف المعلومات التعريفية الشخصية (الصحة - العرق race - الحزب السياسي - المعتقد الديني - التوجه الجنسي - رقم الضمان الاجتماعي - معلومات مالية)،
2. يقدم إشعار قويا بالإضافة إلى إشعار واضح وجلي بفرصة التقيد بجمع أو كشف معلومات التعريف الشخصية.
3. يخطر جميع المستخدمين بتغيير في السياسة المعنية بجمع أو استخدام أو كشف معلومات المستخدم التعريفية الشخصية الحساسة وغير الحساسة.[2]

ويطالب القانون كل مقدم خدمة بتحديد مسؤول الالتزام بالخصوصية

---

(1) Online Personal Privacy Act available at http:// www. techlawjournal.com/ cong107/ privacy/ hollings/ 20020418 summary. asp retrived 122013/6/

(2) Andru E. Wall، Prying Eyes: The Legal Consequences of Reading Your Spouse›s Electronic Mail، 30 FAM. L.Q. (2003) P56

والمسؤول عن تأكيد الالتزام بهذه الجزئية من القانون وغيرها من سياسات الخصوصية.[1]

يقدم القانون استثناءات لمتطلبات الخصوصية بما في ذلك عمليات الكشف الطارئة:

1. والتي تعد حرجة بالنسبة لحياة أو سلامة أو صحة المستخدم أو الأفراد الآخرين.
2. والتي بخصوصها ليس من الممكن الحصول على الموافقة المسبقة.
3. والتي لا تزيد في نطاقها عما هو ضروري لإنجاز الغرض الطارئ.[2]

يطالب القانون من مقدم الخدمة:

1. أن يسمح بدخول مناسب للمستخدم على معلومات التعريف الشخصية التي يتم جمعها والاحتفاظ بها.
2. أن يضع ويحافظ على إجراءات لحماية تأمين وسرية وتكامل مثل هذه المعلومات.

وكذلك - يقدم ما يساعد على تطبيق هذا القانون من خلال مفوضية التجارة الفيدرالية والتي ترى عمليات أو ممارسات الانتهاك غير العادلة أو من الأعمال الخداعية.

يفترض القانون الالتزام بمتطلبات هذا العنوان إذا ما كان مقدم الخدمة:

1. أحد المشاركين في برنامج التنظيم الذاتي المعتمد من قبل مفوضية التجارة الفيدرالية.

---

(1) The Online Personal Privacy Act 2002، Sen. Ernest، reports، Office of Sen. Hollings،(2002) p. 5

(2) Virginia A Jones،Requirements for Personal Information Protection، Part 1: U.S. Federal Law، CRM، FAI، 2008 P72

2. قد تم اعتماده من قبل هذا البرنامج على أنه من الملتزمين تماما.

ويطالب القانون باعتماد مفوضية التجارة الفيدرالية لمثل هذه البرامج التي توفر حماية الخصوصية وفقا للعنوان الأول. كما يطالب مفوضية التجارة الفيدرالية بأن تعيد تقييم موافقتها على كل برنامج كل عامين. كما يسمح القانون بمطالبة مفوضية التجارة الفيدرالية باتخاذ قرار بعدم اعتماد أحد البرامج.(1)

و يكون هذا القانون غير مطبق أو عملي بالنسبة للشركات التجارية الصغيرة التي:

1. يقل عائدها السنوي عن مليون دولار.
2. لديها عدد عاملين أقل من 26 عاملا.
3. تجمع أو تستخدم معلومات التعريف الشخصية من أقل من 1000 مستهلك في العام لغرض لا يرتبط بمعاملات المستهلك المنتظمة.
4. لا تقوم بمعالجة المعلومات التي يتم جمعها.
5. لا تبيع أو تكشف مثل هذه المعلومات للنظر فيها.

و يصرح القانون باتخاذ إجراءات تطبيق القانون من قبل المستخدمين الخصوصيين والولايات نيابة عن المقيمين فيها. ويسمح القانون بتدخل مفوضية التجارة الفيدرالية بالتدخل في إجراءات الولاية.

وكذلك يوفر القانون عمليات حماية للمبلغين عن موظفي مقدمي الخدمة.

---

(1) (1)Charlene Brownlee and Blaze D. Waleski ()Privacy Law،، Law Journal Press، New York، 2006، 2008، page 5 - 56.

بالنسبة للتطبيق بمجلس النواب والوكالات الفيدرالية - يطالب القانون رقيب الأسلحة Sergeant at Arms بمجلس الشيوخ الأمريكي بوضع اللوائح التي تحكم استخدام مسؤولي وموظفي مجلس الشيوخ للإنترنت وفقا لهذا القانون. وينطبق هذا القانون على كل وكالة فيدرالية تعد من مقدمي خدمة الإنترنت أو مقدمي خدمات على الإنترنت أو التي تقوم بتشغيل المواقع باستثناء التطبيق الذي يعرض للخطر أنشطة تطبيق القانون أو التحريات أو الأمن أو عمليات السلامة.(1)

وقد أوضح هذا القانون بعض التعريفات

و يطالب القانون مفوضية التجارة الفيدرالية ب (1) بدء واستكمال وضع قواعد لتنفيذ هذا القانون، و(2) أن تقوم بإبلاغ لجان محددة في مجلس الشيوخ بعمليات التنفيذ وفعالية التنفيذ.

ويعدل قانون المعهد القومي للمعايير والتكنولوجيا National Institute of Standards & Technology لتوجيه المعهد القومي للمعايير والتكنولوجيا بتشجيع ودعم تطوير برامج أو بروتوكولات أو برمجيات الحاسب الآلي القابلة للتركيب على أجهزة الحاسب الآلي، والتي تتيح الدخول على الإنترنت والتي سوف تقوم تلقائيا بتنفيذ برنامج لحماية معلومات التعريف الشخصية أو غيرها من المعلومات الحساسة المعنية بالخصوصية.

العنوان الخامس: الخصوصية حال عدم الدخول على الإنترنت Offline Privacy – يطالب رئيس مفوضية التجارة الفيدرالية بالتقدم إلى لجان مجلس الشيوخ المحددة بتوصيات ولوائح مقترحة حول معايير

(1) Peter P. Swire، Information Privacy، Official Reference for the Certified Information Privacy Professional (CIPP)،

CIPP and Sol Bermann، CIPP، International Association of Privacy Professionals2007، page 29

حماية مماثلة للكيانات التي تقوم بجمع معلومات تعريف شخصية باستخدام أساليب أو إجراءات لا يغطيها هذا القانون.[1]

ومما سبق نخلص إلى أن هذا القانون يعد وعاءً لقوانين خصوصية المستهلك على الإنترنت الأمريكية إذ أنه يعد نتاجا لتسلسل قوانين خصوصية المعلومات إضافة إلى مراعاته لأساليب جمع ومعالجة البيانات سواء على الإنترنت أو على أجهزة الحاسب الآلي مما يفرض للمعلومات والبيانات الحماية اللازمة والمطلوبة منها.

أما بالنسبة للاستثناءات التي قدمها القانون والتي تتعلق بالظرف الطارئ نجد أنه من الممكن إساءة استخدام هذا الاستثناء في الإفصاح عن البيانات والمعلومات الأمر الذي يتطلب فرض رقابة صارمة إثر تطبيق هذا الاستثناء.

---

(1) Cormick، Michelle. "New Privacy Legislation." Beyond Numbers، ProQuest. 2003 P 21

الفرع الثامن

قانون تحديث قانون الخصوصية لمواكبة عصر المعلومات لسنة 2011

The Privacy Act Modernization for

the Information Age Act of 2011[1]

في الثامن عشر من أكتوبر 2011، قدم السيناتور دانيال أكاكا من هاواي مشروع قانون تحديث قانون الخصوصية لأجل مواكبة عصر المعلومات لسنة 2011 إلى مجلس الشيوخ، ويأتي قانون تحديث قانون الخصوصية لأجل مواكبة عصر المعلومات وليدا "للتوسع في التكنولوجيا وانتشار معلومات التعريف الشخصية في أيدي الوكالات الحكومية" لأجل تحديث قانون الخصوصية بسبعة طرق مختلفة:[2]

- يوضح قانون تحديث قانون الخصوصية لأجل مواكبة عصر المعلومات عدة تعريفات لقانون الخصوصية.
- يحدث قانون تحديث قانون الخصوصية لأجل مواكبة عصر المعلومات الاستثناءات فيما يخص متى لا يتوجب على الوكالات إخطار الأفراد بعمليات الإفصاح عن السجلات.
- يحدث قانون تحديث قانون الخصوصية لأجل مواكبة عصر المعلومات متطلبات قانون الخصوصية الخاصة بالكيفية التي تنشر بها الوكالات إشعارات بشأن نظم السجلات.

---

(1) The Privacy Act Modernization for the Information Age Act of 2011 available at https://www.govtrack.us/congress/bills/112/s1732/text retrived 122013/5/

(2) Privacy Act Modernization for the Information Age Act of 2011، http://www.opencongress.org/bill/s1732 - 112/show retrived at 25 - 12 - 2013 P.34

- يعـزز قانـون تحديـث قانـون الخصوصيـة لأجـل مواكبـة عـصر المعلومـات العقوبـات المدنيـة والجنائيـة للإفصـاح الغـير ملائـم للمعلومـات.

- يفضـل قانـون تحديـث قانـون الخصوصيـة لأجـل مواكبـة عـصر المعلومـات تعريـف قانـون الخصوصيـة الحـالي لمعلومـات التعريـف الشـخصية (Personally Identifiable Information (PII.

- يبتـدع قانـون تحديـث قانـون الخصوصيـة لأجـل مواكبـة عـصر المعلومـات وظيفـة كبـير مسـؤولي الخصوصيـة الفيـدرالي Federal Chief Privacy Officer بمكتـب الإدارة والميزانيـة.

- يتوسـع قانـون تحديـث قانـون الخصوصيـة لأجـل مواكبـة عـصر المعلومـات في سـلطة التحـري الممنوحـة حاليـا لإدارة كبـار مسـؤولي الخصوصيـة بأمـن البـلاد لتمنـح لمسـؤولي الخصوصيـة بالـوكالات الأخـرى.[1]

ويـري الباحـث أن هـذا القانـون لم يعـدل مـن المبـادئ الأساسية التـي أرسـتها القوانـين السـابقة إلا أنـه يـدق ناقـوس الإنـذار لبعـض التطـورات التكنولوجيـة، ومنـح الجهـات المسـؤولة سـلطة أوسـع في مراقبـة حمايـة البيانـات، بـل أوصى بإعـادة النظـر في تعريـف بيانـات التعريـف الشـخصي وتوسـيع مجالهـا بمـا يتواكـب مـع العـصر.

---

(1) Annual Report on the Administration of thePrivacy Act 2011 - 2012 available at http:// www. esdc. gc. ca/ eng/ transparency/ ati/ reports/annual_privacy/2011_2012/index.shtml retrived 162013/5/

المطلب الثاني

القوانين التي تحكم خصوصية البيانات في المملكة المتحدة

بعد البحث في القوانين التي تحكم الخصوصية في الولايات المتحدة سوف يتم البحث في القوانين التي تحكم الخصوصية في المملكة المتحدة.

- حيث نجد أن هناك تشريعا رئيسا وهو المصادقة على اتفاقية حقوق الإنسان المعروف بقانون حقوق الإنسان لعام 1998(**الفرع الأول**).
- بالإضافة إلى قانون حرية المعلومات لعام 2000 (**الفرع الثاني**).

الفرع الأول

قانون حقوق الإنسان لعام 1998

(المصادقة على اتفاقية حقوق الإنسان الأوروبية)

قانون حماية البيانات لسنة 1998 هو قانون صادر عن البرلمان البريطاني والذي يعرف القانون البريطاني بشأن معالجة بيانات الأفراد الأحياء. وهو التشريع الرئيس الذي ينظم حماية البيانات الشخصية في المملكة المتحدة. وعلى الرغم من أن القانون ذاته لا يشير إلى الخصوصية، فقد تم سن القانون ليجعل القانون البريطاني متوافقا مع توجيهات حماية البيانات الصادر عن الاتحاد الأوروبي في عام 1995 والذي يطالب الدول الأعضاء بحماية الحقوق الرئيسة وحريات شعوبها وحق الخصوصية المتعلق بمعالجة البيانات الشخصية على وجه الخصوص. وفي الممارسة لا ينطبق القانون على الاستخدام المحلي كما في الاحتفاظ بسجل بالعناوين الشخصية على سبيل المثال. ويعرف القانون ثمانية مبادئ لحماية البيانات. ويطالب أيضا الشركات والأفراد بالاحتفاظ بالبيانات الشخصية لأنفسهم.[1]

بدأ قانون حماية البيانات لسنة 1998 في الأول من مارس 2000 حيث معظم أحكامه قد وضعت موضع التنفيذ اعتبارا من 24 أكتوبر 2001. ولقد استبدل القانون قانون حماية البيانات لسنة 1984 وتوسع فيه. والغرض من القانون هو حماية حقوق وخصوصية الأفراد والتأكد من البيانات التي تخص الأفراد لا يتم معالجتها دون معرفتهم وأنه قد تم معالجتها بموافقتهم متى كان ذلك ممكنا.

---

(1) Data Protection Act 1998، Part IV (Exemptions)، Section 36، "Office of Public Sector Information"، accessed 6 September (2007) P.11

ويغطـي القانـون البيانـات الشـخصية المرتبطـة بالأفـراد الأحيـاء ويقـوم بتعريـف فئـة البيانـات الشـخصية الحساسـة والتـي تخضـع لمزيـد مـن الـشروط الصارمـة في معالجتهـا كـما هـو الحـال مـع البيانـات الشـخصية.[1]

ويغطـي قانـون حمايـة البيانـات البيانـات التـي يتـم الاحتفـاظ بهـا في نمـاذج إلكترونيـة كـما ينطبـق أيضـا عـلى البيانـات اليدويـة التـي يتـم الاحتفـاظ بها فيـما يطلق عليـه القانـون بنظـام حفـظ الملفـات المعنيـة relevant filing system.

وفي حـين أن ذلـك قـد يبـدو مقيـدا لفئـات البيانـات غـير الإلكترونية التـي ينطبق عليهـا القانـون، فقـد قـام قانـون حريـة المعلومـات لسـنة 2000 بالتوسـع في تعريفـات البيانـات الشـخصية في قانـون حمايـة البيانـات فيـما يتعلـق بالسـلطات العامـة مثـل اللجنـة الفرعيـة الاستشـارية لعمليـات الأنظمـة System Operations Advisory Subcommittee (SOAS) والتـي ينطبـق عليهـا قانـون حريـة المعلومـات.

والتأثـير الرئيـس لذلـك هـو أنـه منـذ الأول مـن ينايـر 2005 (عندمـا تـم تفعيـل قانـون حريـة المعلومـات) قـام قانـون حمايـة البيانـات بتغطيـة المعلومـات الشـخصية غـير المنظمـة والتـي تحتفـظ بهـا اللجنـة الفرعيـة الاستشـارية لعمليـات الأنظمـة في شـكل يـدوي، أي ليسـت معنيـة بنظـام حفـظ الملفـات، فيـما عـدا البيانـات غـير المنظمة المرتبطـة بالمواعيـد والطـرد والمدفوعـات والنظـام وغـير ذلـك مـن أمـور الأفـراد والتـي تظـل خـارج نطـاق القانـون.[2]

لذلـك لا بـد مـن الافـتراض كقاعـدة عامـة أن قانـون حمايـة البيانـات يغطـي

---

(1) Report،Review of the Implementation of the Human Rights Act،Department of constitutional Affaires،justice rights and democracy 2006 P 8

(2) Bruce Ackland،Data Protection Act - non - compliance widespread،Bruce Ackland، 2001available at http:// www. computer weekly.com/news/ 2240042855/ Data - Protection - Act - non - compliance - widespread

أي بيانات شخصية مرتبطة بفرد يمكن التعرف عليه والمحتفظ بها لدى اللجنة الفرعية الاستشارية لعمليات الأنظمة في أي شكل من الأشكال.

ومع ذلك، تستثنى البيانات اليدوية غير المنظمة من أي سمة من سمات القانون بما في ذلك المبدأ الأول والثاني والثالث والخامس والسابع والثامن من مبادئ حماية البيانات، ومن المبدأ السادس من مبادئ حماية البيانات فيما عدا ما يخص حقوق صاحب البيانات في الدخول على بياناته والمطالبة بتصحيح أو حجب أو حذف أو إلغاء البيانات غير الدقيقة.

يحل قانون سنة 1998 ويدعم تشريعا صدر مبكرا مثل قانون حماية البيانات لسنة 1984 وقانون الدخول على الملفات الشخصية Access to Personal Files Act لسنة 1987.

وفي الوقت ذاته، هدف القانون إلى تنفيذ توجيه حماية البيانات الأوروبية. وفي بعض الجوانب، وخاصة الاتصالات والتسويق الإلكتروني، فقد تم تهذيبه بتشريع لاحق لأسباب قانونية. فقد ألغت لوائح الخصوصية والاتصالات الإلكترونية (توجيه الاتحاد الأوروبي) Privacy & Electronic Communications (EU Directive) Regulations لسنة 2003 مطلب الموافقة لمعظم عمليات التسويق الإلكتروني لتكون "موافقة إيجابية positive consent" كما في وضع إشارة بالموفقة في المربع opt in box. وتستمر الاستثناءات لعمليات تسويق "المنتجات والخدمات المماثلة" للعملاء والمستفسرين والتي يمكن أن يظل مسموحا بها على أساس الاختيار opt out basis.[1]

ولقد تم وضع قانون حماية البيانات لجيرسي Jersey Data Protection Law على غرار القانون البريطاني.[2]

(1) Ron Condon،،Data Protection Act: UK information to avoid DPA fines، uk press، 2013 P51

(2) Wendy Benjamin،Jersey: "Data Protection In Jersey And Other Offshore Jurisdictions" (23 July 2008) p.53، mondaq.com، retrieved 2012 Sep 14

يغطي تعريف القانون "للبيانات الشخصية" أي بيانات يمكن استخدامها لتحديد شخصية فرد حي.

هذا ولا ينظم القانون البيانات مجهولة المصدر أو المجمعة حيث إن عملية إخفاء هوية المصدر أو التجميع قد تم بشكل متقلب وغير ثابت. ويمكن تحديد شخصية الأفراد بوسائل متعددة تشمل اسمهم وعنوانهم ورقم الهاتف أو عنوان البريد الإلكتروني.

وينطبق القانون فقط على البيانات التي يتم الاحتفاظ بها أو ينتوى الاحتفاظ بها على أجهزة الحاسب الآلي (المعدات التي تعمل تلقائيا استجابة لتعليمات تصدر إليها لذلك الغرض) أو التي يتم الاحتفاظ بها في "نظام حفظ ملفات معني بذلك".[1]

في بعض الأحيان يمكن تصنيف حتى كتاب العناوين الورقي "كنظام حفظ ملفات معني بذلك" كما في اليوميات التي تستخدم لدعم الأنشطة التجارية مثل يوميات مندوب المبيعات على سبيل المثال.

و ينشئ قانون حماية البيانات حقوقا لهؤلاء الذين يتم تخزين بياناتهم والمسؤوليات الواقعة على عاتق هؤلاء الذين يقومون بتخزين أو بث تلك البيانات. وللفرد الذي تتم معالجة بياناته الحق في:

- الاطلاع على البيانات التي تحتفظ بها هيئة من الهيئات عنه. ويمكن الحصول على "طلب دخول فرد على البيانات" مقابل رسم رمزي. واعتبارا من شهر يناير 2014، أقصى رسم هو 2 جنيه إسترليني لطلبات تصديق الوكالات المرجعية و50 جنيه إسترليني لطلب الصحة والتعليم و10 جنيه إسترليني للفرد لغير ذلك.

---

(1) "Data Protection Act 1998، Basic interpretative provisions". Office of Public Sector Information. Retrieved 14 March 2014http://www.legislation.gov.uk/ukpga/199829//section/1 p.34

- طلب تصحيح معلومات خاطئة. إذا ما تجاهلت الشركة الطلب، يمكن للمحكمة أن تأمر بتصحيح أو تدمير البيانات وفي بعض الحالات يمكن أن تحكم بتعويض.

- المطالبة بعدم استخدام البيانات بأي شكل من الأشكال والتي من الممكن أن تتسبب في ضرر أو اكتئاب.

- المطالبة بعدم استخدام بياناته في عملية التسويق المباشرة.

تعد اللجنة الفرعية الاستشارية لعمليات الأنظمة مراقب للبيانات فيما يخص البيانات التي تخضع لمسؤوليتها.

وهو ما يعني أن اللجنة الفرعية الاستشارية لعمليات الأنظمة مسؤولة وفقا لقانون حماية البيانات عن القرارات المتعلقة بمعالجة البيانات الشخصية بما في ذلك قرارات وأفعال معالج البيانات الخارجيين والذي يعملون نيابة عن اللجنة الفرعية الاستشارية لعمليات الأنظمة. ويطالب قانون حماية البيانات بضرورة أن يتم تنفيذ المعالجة وفقا لمبادئ حماية البيانات الثمانية.

أولاً: مبادئ حماية البيانات وفقا للقانون:[(1)]

(1) البيانات الشخصية يجب معالجتها بشكل عادل وقانوني:

SOAS ستعمل علي ضمان الحصول علي المعلومات بوضوح تام، وستقوم علي بذل جهود معقولة ومرتبة لضمان مواضيع البيانات المطلوبة؟، لإضافة ما هي وحدة تحكم البيانات المطلوبة؟ وما هو الهدف من استخدام تلك البيانات؟ وما الفترة الزمنية التي ستحفظ فيها تلك البيانات ؟ وأيا من الأطراف الثلاثة سيتم كشف البيانات لهم؟ ومن أجل معالجة عادلة وقانونية ومشروعة البيانات والمعلومات التي لا تكون بيانات شخصية بالغة الدقة

---

(1) The rights of individuals (Principle 6)، ICO.gov.uk، accessed 14 April 2013 p.51

سوف يتم معالجتها فقط من قبل SOAS لو تحقق شرط واحد علي الأقل من الشروط التالية المنصوص عليها في قانون حماية البيانات وقد تم جمعها كما يلي:

1. موضوع البيانات قد أعطى موافقته موافقتها إلي المعالجة.

2. المعالجة ضرورية لعمل عقد مع موضوع البيانات أو اتخاذ خطوات بنظرة ثاقبة نحو الدخول في العقد.

3. المعالجة مطلوبة بموجب إلزام قانوني بخلاف العقد.

4. المعالجة ضرورية لحماية المصالح الحيوية لموضوع البيانات.

5. المعالجة ضرورية لإقامة وإدارة العدل، تأدية الوظائف تحت قوة تشريع، ممارسة مهام ولي العهد أو دائرة حكومية أو أي وظائف ذات طبيعة عامة تمارس في المصلحة العامة.

6. المعالجة ضرورية لمتابعة المصالح المشروعة للـSOAS أو أي من الأطراف الثلاثة ولا تحيز للحقوق والحريات أو المصالح المشروعة لموضوع البيانات.[1]

معالجة البيانات الشخصية بالغة الدقة والحساسية تخضع لقيود أكثر صرامة بموجب قانون حماية البيانات. وتلك المعالجة للبيانات الشخصية بالغة الدقة التي لا يقوم بها سوى SOAS إذا كان واحد علي الأقل من الشروط المذكورة أعلاه، التي تنطبق علي البيانات غير الدقيقة والحساسة قد تم الوفاء بها. وبالإضافة إلى ذلك فإن واحدا على الأقل من الشروط التالية، المنصوص عليها في تشريعات حماية البيانات the Data Protection Act، يجب أيضا أن تتحقق:

---

(1) Michael Cobb، Contributor، The ‹appropriate› way to comply with Data Protection Act 1998، Poul Wettnd،2011 P105

1. يعطـي موضـوع البيانات له أو لها موافقة صريحة.

2. المعالجـة مطلوبـة مـن قبل القانون مع اتصال مـع جهة العمل.

3. المعالجـة ضروريـة لحمايـة المصالـح الحيويـة لموضـوع البيانات أو أي شـخص آخر.

4. إحـراز المعلومات العامة من خـلال موضوع البيانات.

5. يكـون مـن الـضروري القيـام بالمعالجـة أو التجهيـز للإجـراءات القانونيـة، الحصـول عـلي المشـورة القانونيـة أو إنشـاء أو الدفـاع عـلي الحقـوق القانونيـة.

6. تكـون المعالجـة مطلوبـة لإقامـة وإدارة العـدل، ممارسـة الوظائـف تحـت طائلـة القانـون أو ممارسـة مهـام ولي العهـد أو دائـرة حكوميـة.[1]

7. المعالجـة مطلوبـة وضروريـة للأغـراض الطبيـة وتنفـذ مـن قبـل المهنيـن الأطبـاء أو شـخص مـع واجـب يعـادل السريـة.

8. المعالجـة ضروريـة لتحقيـق مبـدأ تكافـؤ الفـرص بـين النـاس في مختلـف الاتجاهـات كالاختـلاف العرقـي أو العنـصري مثـلا أو الاختـلاف في المعتقدات الدينيـة كذلـك، التـدرج في الحالـة الصحيـة البدنيـة أو العقليـة، والتـدرج أيضـا في الظـروف الماديـة أو العقليـة.

9. المعالجـة تعمـل في جوهـر المصلحـة العامـة وضروريـة لمنـع أو اكتشـاف أي عمـل غـير قانـوني وكذلـك أيضـا في حالـة الامتنـاع عـن عمـل شيء أخـر.

---

(1) Report The Guide to Data Protection، How much do I need to know about data protection?.ICO 2006 available at http://ico.org.uk/Global/~/media/documents/library/Data_Protection/Practical_application/THE_GUIDE_TO_DATA_PROTECTION.ashx retrivted 16/6/2013

10. المعالجة أو التجهيز تصب في المصلحة العامة وضرورية لحماية العامة والجمهور من خيانة الأمانة، سوء التصرف، عدم اللياقة وعدم الكفاءة، التصرفات غير اللائقة على محمل الجد، سوء الإدارة في إدارة الخدمات أو الفشل في تلك الخدمات.

11. المعالجة تصب في المصلحة العامة، فهي تشتمل وتنطوي على المعلومات المتعلقة بالنقطة (10) أو النشر لأغراض الصحافة والأدب أو الفن.

12. المعالجة أو التجهيز تصب في المصلحة العامة وتكون ضرورية في الوظائف المتعلقة بخدمة المشورة.

13. المعالجة تعمل في جوهر المصلحة العامة، وضرورية للأغراض البحثية شريطة ألا تدعم المعالجة تدابير أو قرارات فيما يتعلق الأفراد، كما أنها لا تسبب أضرار كبيرة أو محنة لموضوع البيانات أو أي شخص آخر.

تقوم تلك القائمة بحذف بعض الحالات المتعلقة بمعالجة البيانات الشخصية الحساسة والدقيقة والتي تكون من المرجح أنها ليست لها صلة بSOAS

البيانات المتعلقة بذوي الإعاقة من الطلاب وفريق العمل والموظفين وغيرهم من الأفراد تكون بيانات شخصية حساسة ودقيقه جدا، وتقع تحت طائلة قانون حماية البيانات Data Protection Act. ومثل تلك البيانات لابد أن تتم معالجتها بالتوافق مع سياسة الإعاقة في SOAS SOAS's Disability Policy.

(2) البيانات الشخصية يحصل عليها فقط لغرض أو أغراض محدده، مشروطة، مشروعة وقانونية:

وكذلك لا يجوز أن تعالج بأي طريقه أخرى غير متوافقة مع هذا الغرض أو الأغراض [1]

SOAS ستقوم بضمان أن البيانات التي سيتم الحصول عليها لغرض محدد لن يقام استخدامها في غرض آخر مختلف عن المحدد لها. ما لم يتم ذلك الاستخدام إلا بموافقة موضوع البيانات وتلك البيانات ستغطي بوثيقة تسجيل لSOAS مع مفوضيه المعلومات Information Commissioner أو من ناحية أخرى سيسمح بموجب قانون حماية البيانات Data Protection Act.

(3) لابد أن تكون البيانات الشخصية كافية ولها صلة وطيدة ولا يوجد بها إفراط بالنسبة للغرض أو الأغراض التي تكون محل المعالجة:

لن تقوم SOAS بتجميع أي بيانات شخصية غير ضرورية بدرجة كافية للغرض أو الأغراض التي تم الحصول عليها.

(4) البيانات الشخصية المجهزة لابد أن تكون دقيقة وعند الضرورة لابد من تحديثها:

ستقوم SOAS باتخاذ خطوات معقولة لضمان دقة المعلومات الشخصية التي سيتم الاحتفاظ بها. وسوف تتخذ الخطوات اللازمة لتصحيح البيانات غير الدقيقة عند طلب القيام بذلك من قبل صاحب البيانات.

---

(1) J. Morgan، "Privacy، Confidence and Horizontal Effect: "Hello" TroubleCambridge Law Journal 444،2003، P 65

(5) البيانات الشخصية المعالجة لأي غرض من الأغراض لا يجوز لها أن تبقي لفترة أطول مما هو ضروري لهذا الغرض:

SOAS ستضمن أن البيانات الشخصية لن يحتفظ بها لفترة أطول من المطلوب الاحتفاظ بها من أجل الغرض أو الأغراض التي جمعت البيانات من أجلها. من الممكن الإبقاء علي بعض المعلومات من قبل SOAS إلي أجل غير مسمي وذلك لأغراض بحثية (بما في ذلك من أغراض تاريخيه وإحصائية)، علي النحو المسموح به من قبل قانون حماية البيانات Data Protection Act رهنا بالشروط المنصوص عليها في قانون لهذا النوع من المعالجة (الرجاء النظر إلي جزء كيفية استخدام البيانات الشخصية في مجال البحوث).[1]

(6) البيانات الشخصية المعالجة وفقا للحقوق موضوعات البيانات بموجب قانون حماية البيانات:

SOAS ستضمن أن البيانات الشخصية المعالجة تتم بالتوافق مع حقوق مواضيع البيانات بموجب قانون حماية البيانات، وهذه الحقوق تشتمل علي الحق في:

- تقديم طلبات الحصول علي الموضوع (انظر الدخول إلي المعلومات) لمعرفة ما يقام من المعلومات عنهم، والأغراض التي سيتم استخدامها، والذين تم الكشف عنه.
- منع معالجة البيانات التي من المرجح أن تسبب لهم أضرار كبيرة وحقيقة أو ضائقة كبيرة
- منع المعالجة لأغراض التسويق المباشر.
- كن على علم بشأن عمليات اتخاذ القرارات الآلية والتي ستؤثر

(1) H. Fenwick and G. Phillipson، “Confidence and Privacy: A Re - Examination” Cambridge Law Journal 447. 1999 P65

عليهم.

- منع القرارات المهمة التي تؤثر عليهم من تبذل فقط بواسطة العمليات الآلية والأوتوماتيكية.
- إقامة دعوى للتعويض إذا كانوا يعانون الضرر من خلال مخالفة القانون.
- اتخاذ الإجراءات اللازمة لطلب التصحيح، الحجب، المحو أو تدمير البيانات الغير دقيقة.
- طلب إجراء تقييم من قبل مفوض المعلومات من مشروعية أية معالجة ستظهر.

(7) اتخاذ التدابير التقنية والتنظيمية المناسبة للحيلولة دون معالجة غير مصرح بها أو غير مشروعة للبيانات الشخصية وفقدانها، وتدمير أو تلف البيانات الشخصية:

SOAS ستتخذ خطوات لضمان حماية المعلومات الشخصية والتي عقدت إلكترونيا وفي هيئة دليل منسوخ، ولمنع الكشف غير المصرح به للبيانات لأطراف ثالثة، وفقدان أو تلف البيانات التي يمكن أن تؤثر علي مصالح موضوع البيانات. SOAS ستضمن أن معالجة البيانات توفر وتحتاط لأمر الأمن بمستوى مناسب وكاف للبيانات الشخصية والتي تعالج بالنيابة عن SOAS.(يرجي النظر إلي أمن البيانات).

(8) لا يجوز نقل البيانات الشخصية إلى بلد أو إقليم خارج المنطقة الاقتصادية الأوروبية إلا لبلد أو إقليم يضمن مستوى كاف من الحماية للحقوق والحريات من مواضيع البيانات فيما يتعلق بقضية معالجة البيانات الشخصية:

SOAS لن تقوم بنقل بيانات خارج المنطقة الاقتصادية الأوروبية إلا إذا كان ذلك الانتقال مسموح به من قبل قانون معالجة البيانات (انظر إلي نقل المعلومات خارج المنطقة الاقتصادية الأوروبيةEEA) بطلب من قانون حماية

البيانـات، الهيئـات التـي تسـجل وتسـتخدم المعلومـات الشـخصية لتسـجل مـع مفـوض المعلومـات Information Commissioner وتفاصيـل تسـجيل وتوثيـق SOAS يتـم تضمينهـا في سـجل تحكـم البيانات Register of Data Controllers والتي تكون متاحة عـلي الموقـع الإلكـتروني لمفـوض المعلومـات Information Commissioner. فإنه يقوم بتسـجيل الأغـراض والأهـداف التـي مـن أجلهـا جمـع SOAS البيانـات الشـخصية وأنواع مواضيـع البيانـات التـي تغطـي كل غـرض ومسـتويات البيانـات المجمعـة والمسـتلمين الذيـن سـيتم كشـف البيانـات لهـم والبـلاد أو الأقاليـم التي سـيتم نقـل البيانـات لها. أي اسـتخدام للـSOAS للبيانـات الشـخصية لابـد أن تتـم بالتوافـق مـع شروط تسـجيل تلك البيانـات في ال SOAS.

المعلومـات المتعلقـة بكيفيـة معالجـة SOAS للبيانـات المتعلقـة بطلابهـا وارده في بيـان حمايـة البيانـات الطلابية Student Data Protection Statement.

وهـذا يـشرح ويبـين للطـلاب مـا هـي المعلومـات التـي تجمعهـا عنهـم المدرسـة، كيـف سـيتم اسـتخدام المعلومـات الخاصـة بهـم بواسـطة SOAS بينـما هـم طـلاب في المدرسـة وبعـد أن يتخرجـوا منهـا، مـا هـي الـوكالات الخارجيـة التي قـد تتلقـي بياناتهم ومعلوماتهـم، ومـا هـي حقوقهـم ومسـؤوليتهم في مـا يتعلـق بتلـك البيانات. ذلـك البيان يتسـع لمزيـد مـن المعلومـات العامـة عـن معالجـة البيانـات الشـخصية الـواردة في تلـك السياسة.[1]

باســتثناء الاســتثناءات المذكــورة فيــما بعــد، يحتــاج الفــرد إلى الموافقــة عــلى جمــع معلوماتــه الشــخصية واســتخدامها في الغــرض أو الأغــراض المطلوبــة. ويعــرف التوجيــه الأوروبي لحمايــة المعلومــات European Data Protection Directive الموافقـة عـلى أنهـا "... أي إشـارة صريحـة تعطـي تحديـدا أو للإفـادة

---

(1) Fenwick and G. Phillipson، "Breach of Confidence as a Privacy Remedy in the Human Rights Act Era" (2000) Modern Law Review 660. P 63.

بالعلـم عـن رغبتـه والتـي بهـا يبـين صاحـب البيانـات موافقتـه عـلى أن يتـم معالجـة بياناتـه الشـخصية"، مـما يعنـي أنـه يمكـن للفـرد أن يعـبر عـن موافقتـه بغـير الكتابـة. ومـع ذلـك، يجـب عـدم تفسـير عـدم التواصـل عـلى أنـه موافقـة.[1]

وبالإضافـة إلى ذلـك، يجـب أن تكـون الموافقـة متناسـبة مـع عمـر وأهليـة الفـرد ومـع ظـروف الحالـة الأخـرى. فعـلى سـبيل المثـال، إذا مـا "انتـوت" هيئـة "الاسـتمرار في الاحتفـاظ بالبيانـات الشـخصية أو اسـتخدامها بعـد نهايـة العلاقـة مـع الفـرد، فإنه يجب حينئـذ أن تغطـي الموافقـة ذلـك".

وحتـى إذا مـا تـم إعطـاء الموافقـة، يجـب عـدم افـتراض أنهـا سـتدوم إلى مـا لا نهايـة. فعـلى الرغـم مـن أنـه في معظـم الحـالات تـدوم الموافقـة بقـدر مـا تتطلـب البيانـات الشـخصية الخضـوع للمعالجـة، فـإن بإمـكان الأفـراد سـحب موافقتهـم تبعـا لطبيعـة الموافقـة والظـروف التـي تـم فيهـا جمـع المعلومـات الشـخصية واسـتخدامها.

كـما يحـدد قانـون حمايـة البيانـات أيضا أنـه يتوجب معالجـة البيانات الشـخصية الحساسـة وفقـا لمجموعـة متشـددة مـن الـشروط مـع ضرورة أن تكون الموافقـة صريحة عـلى وجـه الخصوص.

ثانياً:الاستثناءات:

لقـد تـم هيكلـة القانـون بحيـث إن جميـع عمليـات معالجـة البيانـات الشـخصية تكـون مغطـاة بالقانـون في حـين أنـه أتـاح عـدد مـن الاسـتثناءات في الجزء الرابـع. وأبرز الاسـتثناءات هـي:

- الأمـن القومـي تسـتثنى أي معالجـة لغـرض حمايـة الأمـن القومـي مـن كافـة مبـادئ حمايـة البيانـات إلى جانـب الجـزء الثـاني (حقـوق دخـول صاحـب البيانـات عـلى بياناتـه)، والجـزء الثالـث (الإشـعار) والجـزء

(1) R. Singh and J. Strachan، "Privacy Postponed" European Human Rights Law Review[2003] P 12 - 25

الخامس (التطبيق) والقسم 55 (الحصول غير القانوني على البيانات الشخصية.

- الجريمة والضريبة - تستثنى البيانات المعالجة لأجل منع أو كشف الجريمة أو القبض على المدعى عليهم ومحاكمتهم أو تقييم أو جمع الضرائب من المبدأ الأول لحماية البيانات.

- الأغراض المحلية تستثنى المعالجة التي تتم بمعرفة الفرد فقط وللأغراض الشخصية للفرد أو العائلة أو الشؤون المنزلية من جميع مبادئ حماية البيانات إلى جانب الجزء الثاني (حقوق دخول صاحب البيانات على بياناته) والجزء الثالث (الإشعار)،[1] و يفصل القانون عددا من الجرائم المدنية والجنائية التي قد يتعرض لها مراقبي البيانات إذا ما فشل مراقب البيانات في الحصول على الموافقة المناسبة من صاحب البيانات. ومع ذلك، لم يتم تعريف "الموافقة" بشكل محدد في القانون، لذلك، فإن الموافقة تعد من أمور القانون العام common law.

- فمثلا معالجة المعلومات الشخصية دون تسجيل تعد من الجرائم.

- إن عدم الالتزام بلوائح الإشعار التي يضعها وزير الخارجية (والتي يقترحها مفوض المعلومات) تعد من الجرائم.

- يعتبر هذا القسم أن الحصول على المعلومات الشخصية بصورة غير قانونية. يعتبر هذا القسم أن الأفراد (الأطراف الأخرى) مثل قراصنة الإنترنت (الهاكرز hackers) والمقلدين من خارج الهيئة الساعين إلى الحصول على دخول غير مشروع على البيانات الشخصية تعد من الجرائم.

---

(1) Vinod Bange and Graham Hann An overview of UK data protection law، Taylor Wessing،2006 P 9

- يعتبر هـذا القسـم أن مطالبـة الفـرد بتقديم طلـب دخول لصاحـب البيانات يرتبـط بالتحذيـرات أو الإدانـات لأغـراض التعيـين أو الاسـتمرار في العمـل أو مـن بنـود الخدمـات يعـد مـن الجرائـم الجنائيـة. ولقـد تـم تفعيـل ذلـك بقانـون حمايـة البيانـات لسـنة 1998.[1]

و يعـرف هـذا القانون البيانات الشـخصية بأنها:

البيانات الشخصية هي البيانات التي ترتبط بفرد حي يمكن التعرف عليه:

- مـن تلك البيانات، أو
- مـن تلـك البيانـات والمعلومـات الأخـرى المتوافـرة في حـوزة أو مـن المحتمـل أن تكـون في حـوزة مراقـب البيانـات.

وتتعلـق البيانـات الشـخصية الحساسـة بعرقيـة أو الميـول السياسـية أو ديانـة أو وضـع النقابـة المهنيـة أو الصحـة أو الحيـاة الجنسـية أو السـجل الجنـائي لصاحـب البيانـات.[2]

وفقـا للقانـون، يجـوز رفـض طلبـات دخـول صاحـب البيانـات عـلى البيانـات الشـخصية التـي عـادة مـا يتـم الاحتفـاظ بهـا لمـدة تقـل عـن 40 يومـا. ويرجـع ذلـك إلى الحـد الزمنـي الـذي يتوجـب عـلى مراقبـي البيانات اسـتيفاؤه عنـد عرض ردهـم. فإذا ما كان قـد تـم حـذف البيانـات وفقـا للإجـراءات المعتـادة للعمـل في الوقـت الذي يـرد فيه مراقـب البيانـات عـلى طلـب صاحـب البيانـات، فإنـه في هذه الحالـة لن يكـون بالإمكان تقديـم البيانـات. وبالنسـبة لبيانـات مثـل صـور الدوائـر التليفزيونيـة المغلقـة والتـي يتـم الكتابـة عليهـا، فقـد يكـون مـن المسـتحيل عـلى صاحـب البيانـات ممارسـة حقـه في الدخـول عـلى بياناتـه.

(1) Litman، Jessica Digital Copyright. Berlin: Prometheus Books.2000 p. 208.

(2) Duke،Privacy: The Development of a Law and the Legal Theory، UK BOOKs،، 2011 P 163

وتتـولى سـلطة مسـتقلة متمثلـة في مكتـب مفـوض المعلومـات Information Commissioner's Office والتـي يتوافـر لديهـا التوجيهـات المرتبطـة بالقانـون تنظيـم وتطبيـق الالتـزام بالقانـون.

و مـن هنـا نخلـص إلى أن قانـون حمايـة البيانـات البريطـاني قانـون متسـع يحظى بسـمعة التعقيـد. ففـي حـين أنـه يتـم احـترام المبـادئ الأساسـية لحمايتهـا الخصوصيـة، فـإن تفسـير القانـون ليـس دومـا بالأمـر البسـيط. فكثير مـن الـشركات والهيئـات والأفراد يبقـون غـير متأكديـن تمامـا مـن أهـداف ومحتـوى ومبـادئ قانـون حمايـة البيانات.

ويتخفـى البعـض خلـف القانـون فيرفضـون تقديـم المادة المتاحـة الرئيسـة المعلنة حيـث يصفـون القانـون بالقيـد. كـما يؤثـر القانـون أيضـا عـلى الطريقـة التـي تديـر بهـا الهيئـات أعمالهـا مـن حيـث مـن الـذي يمكـن الاتصـال بـه لأغـراض التسـويق ليـس فقط عـن طريـق الهاتـف والبريـد المبـاشر، بـل أيضـا بالوسـائل الإلكترونيـة مـما أدى إلى وضع إسـتراتيجيات تسـويق قائمـة عـلى الحصـول على الإذن.

ويحـدد القانـون تعريفـا محـدداً للبيانـات الشـخصية إلا أنـه لا يفـرض الحمايـة إلا للبيانـات التـي تتـم تدولهـا عـبر وسـيط إلكـتروني ومـن ثـم فـإذا مـا تـم طبـع مثـل البيانـات فإنهـا لا تحظـى بالحمايـة.

وبالرغـم مـن هـذا فيعـد هـذا القانـون الإطـار الأسـاسي لحمايـة البيانـات والمعلومـات في المملكـة المتحـدة لكونـه يشـمل عـلى المبـادئ الأساسـية بالرغـم مـن تعقيـده.

الفرع الثاني

قانون حرية المعلومات لعام 2000 [1]

قانون حرية المعلومات 2000 هو أداء برلماني يقوم به البرلمان في المملكة المتحدة حيث إنه يخلق ويحق للعامة "حق الدخول" إلي المعلومات التي تحتفظ بها السلطات العامة.

وهو تنفيذ لقانون حرية المعلومات في المملكة المتحدة على المستوى الوطني، وهو قانون ينفذ بيان التزام لحزب العمال في الانتخابات العامة 1997 والذي قام بوضعه د. ديفيد كلارك Dr David Clark وظهر في الجريدة البيضاء White Paper عام 1997.

ويعتقد أن الصيغة النهائية للقانون قد تكون أضعف من تلك المقترحة في حين كان العمل في المعارضة. وجاءت الأحكام الكاملة للعمل حيز التنفيذ في 1 يناير 2005.[2]

القانون مسؤولية قسم اللورد شانسيلوورس Lord Chancellor's Department (اسمها الآن وزارة العدل) وهذا القانون أدى لإعادة تسمية مفوض حماية البيانات Data Protection Commissioner والتي أنشئت لإدارة قانون حماية البيانات(Data Protection Act) والذي يعرف الآن بمفوض المعلومات Information Commissioner.

(1) "The Freedom of Information Act 2000 (Commencement No. 1) Order 2001". Statutory Instrument. Ministry of Justice

(2) "Independent Review of the impact of the Freedom of Information Act: A REPORT PREPARED FOR THE DEPARTMENT FOR CONSTITUTIONAL AFFAIRS"، Frontier Economics Ltd، October 2006. Retrieved on 2012 - 05 - 28

مكتـب مفـوض المعلومـات تـشرف عـلى العمليـة القانونيـة The Office of the Information Commissioner oversees the operation of the Act.

القانـون الثـاني لحريـة المعلومـات خـرج للنـور في المملكـة المتحـدة، حريـة المعلومـات (إسـكتلندا) القانـون 2002 (النـاشر 13) Freedom of Information (Scotland) Act 2002 (asp 13)). صـدر مـن قبـل البرلمـان الإسـكتلندي في عـام 2002 لتغطيـة الهيئـات العامة المسـؤول عنهـا البرلمان هوليـوود Holyrood Parliament بدلا مـن وستمنسـتر Westminster في الولايـة. لتلـك المؤسسـات، فإنـه يحقـق نفـس الغـرض باسـم قانـون 2000.

يتـم إجـراء حـوالي 120،000 طلـب كل عـام. المواطنـون مـن لهـم طبيعـة خاصـة وحدهـم لديهـم 60% مـن تلـك الطلبـات، مـع الـشركات والصحفيـين يمثلـون 20٪ و10٪ عـلى التعاقـب. طلبـات الصحفيـين اسـتغرقت أكـثر مـن الوقت الرسـمي لطلبـات الهيئات والأفـراد وقـد تكلف هـذا القانـون £ 35500000 في عـام 2005.[1]

القانـون ينفـذ البيـان الصـادر عـن حـزب العمال في سـنة 1997 خـلال الانتخابات العامـة. قبـل الأخـذ بهـذا القانـون لم يكـن هنـاك أي الحـق في الوصـول إلى الحكومـة من قبـل الجمهـور العـام، مجـرد إطـار تطوعي محـدود لتبـادل المعلومات.

قـدم هـذا القانـون سـنة 1998 في الجريـدة البيضـاء، بعنـوان "حقـك في المعرفـة" بقلـم د. ديفيـد كلارك "Your Right to Know" by Dr David Clark.

(1) "Independent Review of the impact of the Freedom of Information Act: A REPORT PREPARED FOR THE DEPARTMENT FOR CONSTITUTIONAL AFFAIRS"، Frontier Economics Ltd، (October 2006) p.34

وقد استقبلت تلك الجريدة عند إصدارها بحماسة وحفاوة بالغة جدا علي نطاق واسع، ووصفت علي أنها "أقرب ما تكون جيدة لتكون صحيحة"، من قبل أحد الدعاة لحرية تشريع المعلومات. القانون النهائي كان إلى حد كبير أكثر محدودية في النطاق من الورقة البيضاء الأولي.[1]

مشروع القانون أصدر في مايو 1999 وقد نوقش القانون على نطاق واسع في مجلس العموم ومجلس اللوردات House of Commons and the House of Lords، وتلقت الموافقة الملكية في نوفمبر 2000.

ينشئ قانون حرية المعلومات حق قانوني للدخول على المعلومات فيما يتعلق بالأجهزة التي تمارس وظائف ذات طبيعة عامة، ويغطي القانون ثلاثة أنواع من الأجهزة المختلفة. السلطات العامة Public Authorities والشركات المملوكة ملكية عامة وأجهزة محددة تؤدي وظائف عامة.[2] وهي كالتالي:

أولاً: السلطات العامة:

من حيث المبدأ، ينطبق قانون حرية المعلومات على جميع "السلطات العامة" داخل المملكة المتحدة، قائمة كاملة "بالسلطات العامة" لأغراض هذا القانون. وتضم القائمة التي تتراوح من مجلس رفاهية حيوانات المزارع إلى مجلس الشباب لأيرلندا الشمالية من الإدارات الحكومية ومجلس النواب ومؤتمر أيرلندا الشمالية ومؤتمر ولش والقوات المسلحة وأجهزة الحكومة المحلية وأجهزة الخدمات الصحية الوطنية والمدارس والكليات والجامعات وسلطات الشرطة وقائد الشرطة. ولقد تم استبعاد عدد قليل من الوزارات الحكومية صراحة من نطاق القانون وتحديدا خدمات الاستخبارات.

(1) Hazel، Robert. "Commentary on The Freedom of Information White Paper، unit - publications (2013) p.156

(2) "Every expense spared"، The Economist، 19 December 2006، Number 8532، p. 46. Retrieved on 2013 - 07 - 20.

ونظـرا لأن الإدارات الحكوميـة تغلـق وتنشـأ، لـذا يجـب أن يتـم تحديـث القانون بشـكل مسـتمر. ويمنح القسـم الرابـع وزيـر الدولـة Secretary of State للشـؤون الدسـتورية سـلطة إضافـة أي جهـاز أو شـاغل أحـد المناصـب officeholder إلى الجدول رقـم 1 كسـلطة عامـة إذا مـا كانـوا ينشـئون قانونـا أو امتيـازا، كـما أن الحكومـة تقـوم بتعيـين أعضائهـا.

مـن المهـم ملاحظـة أن للقانـون تأثـير محـدود عـلي بعـض السـلطات العامـة. فعـلى سـبيل المثـال، تخضـع هيئـة الإذاعـة البريطانيـة BBC للقانـون فقـط فيـما يخـص المعلومـات التـي لا يتـم الاحتفـاظ بهـا للأغـراض الصحفيـة أو الفنـون أو الأدب لتجنـب تعـرض أنشـطتها الصحفيـة لفضائـح محتملـة. ولقـد تـم النظـر في نطـاق هـذا البنـد في قـرار حديـث للمحكمـة العليـا في قضيـة هيئـة الإذاعـة البريطانيـة BBC ضـد شـوجر Sugar وهـى وثيقـة داخليـة لهيئـة الإذاعـة البريطانيـة تفحـص تغطيـة هيئـة الإذاعـة البريطانيـة للـشرق الأوسـط عـلى خلفيـة احتـمال وجـود تحيـز.

ولقـد جـادل المسـتأنفين في هـذه القضيـة عـلى أن الوثيقـة قـد تـم إعدادهـا لأسـباب معلوماتيـة وصحفيـة وبالتـالي، فإنـه يجـب عـدم تغطيتهـا بالإعفـاء الجزئي الذي ينصـه القانـون. إلا أن المحكمـة العليـا رفضـت تلـك الحجـة ورأى السـيد القـاضي إيروين أن معنـى الصحافـة في القانـون يعنـي أن أيـا مـن المعلومـات التـي يتـم الاحتفـاظ بهـا لمثـل هـذه الأغـراض كان يشـملها الإعفـاء. [1]

ومـا اسـتخلصه هـو أن الكلـمات بالجـدول تعنـي أنـه ليـس عـلى هيئـة الإذاعـة البريطانيـة أي التـزام نحـو كشـف المعلومـات التـي لديهـا، ولأي مـدى لأغـراض الصحافة أو الفـن أو الأدب وسـواء كانـت المعلومـات يتـم الاحتفـاظ بهـا لأغـراض أخـرى أم لا.

والكلـــمات لا تعنـــي أن تلـــك المعلومـــات قابلـــة للكشـــف إذا مـــا تـــم

(1) Hopwe،M، E A Short Guide to the Freedom of Information Act and Other New Access Rights The Campaign for Freedom of Information، 2010 P 2

الاحتفاظ بها لأغراض مختلفة عن الصحافة أو الفنون أو الآداب في حين أنه يتم الاحتفاظ بها أيضا لأي مدى للأغراض المدرجة في القائمة.

أما إذا كان يتم الاحتفاظ بالمعلومات لأغراض مختلطة بما في ذلك لأي مدى فإن الأغراض المدرجة في الجدول أو لأحد هذه الأغراض، فإن المعلومات لا تكون قابلة للكشف.

أيدت الأغلبية في المحكمة العليا (مع اعتراض اللورد ويلسون) هذا القرار وقد أشاروا إلى ضرورة أن يتم استثناء الكشف عن أية معلومات يتم الاحتفاظ بها لأغراض الصحافة أو الفنون أو الآداب حتى لو كان الاحتفاظ بالمعلومات في الغالب لأغراض أخرى.[1]

ثانياً: الشركات المملوكة ملكية عامة:

الشركات التي تندرج ضمن تعريف الشركات المملوكة ملكية عامة تحت القسم السادس من القانون تقع تلقائيا ضمن إطار القانون. وينص القسم السادس على أن الشركة تكون ملكية عامة إذا كانت:

1. مملوكة كاملة للتاجر
2. مملوكة كاملة لسلطة عامة.
3. إدارة حكومية.
4. أي سلطة مدرجة فقط فيما يتعلق بمعلومات معينة[2].

ثالثاً:الأجهزة المحددة:

وفقا للقسم الخامس من القانون، يجوز لوزير الخارجية أن يحدد المزيد

---

(1) Kettle، Martin "World exclusive Tony Blair interview". The Guardian (London) (1 September 2010).P 26.

(2) John Waddam،Kelly Harres،Blackstone›s Guide to the Freedom of Information Act 2000 oxford University press،2010 P 205

مـن الأجهـزة كسـلطات عامـة وفقـا للقانـون شريطـة أن تكـون تلـك الأجهـزة تمـارس وظائـف ذات طبيعـة عامـه أو متعاقـدة لتقديـم خدمـة بنودهـا وظيفـة ذات سـلطة عامـة.

ولقـد توسـع الأمـر الأول وفقـا للقسـم الخامـس (في نوفمـبر 2011) في القائمـة لتشـمل أيضـا رابطـة كبـار ضبـاط الشرطـة Association of Chief Police Officers، ودائـرة المظـالم الماليـة Financial Ombudsman Service وخدمـة الالتحـاق بالجامعـات والكليـات University & College Admission Service.

وينشـئ القانـون حقـا عامـا للدخول عـلى المعلومـات التـي تحتفظ بها السـلطات العامـة بطلـب يتـم التقـدم بـه. ومتـى تـم اسـتلام المطالبـة بحريـة المعلومـات، يصبـح أمـام السـلطة العامـة واجبان:

الأول: واجـب نحـو إخطـار أحد أعضـاء العموم بمـا إذا كانت تحتفـظ بالمعلومات المطلوبـة أم لا (وفقا للقسـم الفرعي الأول (1)(أ)):

وثانيـا: إذا مـا كانـت تحتفـظ بتلـك المعلومـات، فسـوف تبلغهـا للشـخص المتقدم بالطلـب (وفقا للقسـم الفرعـي الأول (1)(ب)).

وبذلـك، يمنـح القانـون حقـوق متسـاوية بالتأكيـد أو الرفـض وتوصيـل المعلومات المعنيـة للفـرد الـذي يتقـدم بالطلـب وفقـا للقانـون. ويكمـل الواجـب الرئيـس واجـب إضـافي بمسـاعدة الأفـراد في كيفيـة التقـدم بطلبـات والتأكـد مـن أنهـم يصيغـون طلباتهم الخاصـة بحريـة المعلومـات بشـكل مناسـب (القسـم الفرعـي الأول (1)).

ومـع ذلـك، هنـاك العديـد مـن الاسـتثناءات بعضهـا يمثـل موانـع مطلقـة عـن الكشـف عـن المعلومـات، بعضهـا تقديـري مـما يعنـى أن للسـلطة العامـة أن تقـرر مـا إذا كانـت المصلحـة العامـة في الكشـف عـن المعلومـات المعنيـة تفـوق المصلحـة العامـة في التمسـك بالاسـتثناء. فالمتقـدم بطلـب للحصـول عـلى معلومـات والـذي

يـرى أن الطلـب قـد تم رفضه بشـكل خاطئ، يمكنـه التقدم بطلب إلى مفـوض المعلومات والـذي لديـه سـلطة الأمـر بكشـف المعلومـات. ومـع ذلـك، فـإن مثـل هـذه الطلبـات يمكـن الاسـتئناف بشـأنها لـدى محكمـة متخصصـة (محكمـة المعلومـات Information Tribunal) وفي بعـض الأحيـان يكـون لـدى الحكومـة السـلطة لتجـاوز أوامـر مفـوض المعلومـات.

يمكـن لأي شـخص أن يطلـب معلومـات وفقـا للقانـون، ويشـمل ذلـك الكيانـات القانونيـة مثـل الـشركات. وليـس هنـاك نموذج خـاص لطلـب المعلومـات. ولا يحتـاج المتقدمـون بطلبـات إلى الإشـارة إلى القانـون عنـد كتابتهـم للطلـب. كـما لا يحتـاج المتقدمـون بطلبـات إلى إعطـاء أسـباب لتقدمهـم بطلـب المعلومـات.

الاستثناءات:[1]

عـلى الرغـم مـن أن القانـون يغطـي مجـال واسـع مـن المعلومـات الحكوميـة، فإن القانـون يحـوي أحكامـا متنوعـة تقـدم اسـتثناء مـن الكشـف عـن نوعيـات محـددة مـن المعلومـات. فالقانـون يحتـوى عـلى شـكلين من الاسـتثناءات:

- اسـتثناءات "مطلقـة" والتـي لا تخضـع لأي تقييـم للمصلحـة العامـة، وتمثـل موانـع "مطلقـة absolute" للكشـف عـن المعلومـات.
- واسـتثناءات "تقديريـة qualified" يؤخـذ خلالها المصلحـة العامة في الاعتبار وموازنـة المصلحـة العامـة في الاحتفـاظ بالمعلومـات في مقابـل المصلحـة العامـة في الكشـف عـن المعلومـات. ولقـد اقترحـت الورقـة البيضـاء الأصليـة للحكومـة حـول قانـون حريـة المعلومـات سـبع فقـط من تلـك الاسـتثناءات، إلا أن مـشروع القانـون النهـائي تضمـن 24 اسـتثناء.

(1) "Lord Williams of Mostyn Memorial Lecture"، L.Williams،ukorg publications،20011

الاستثناءات المطلقة Absolute Exemptions:

الاستثناءات التي يطلق عليها "الاستثناءات المطلقة" لا تقدير للمصلحة عامة المرتبطة بها، ويحوي القانون ثمانية من تلك الاستثناءات:

- المعلومات التي يتم الدخول عليها بوسائل أخرى (القسم 21).
- المعلومات المرتبطة بأمور الأمن أو التي تتناول أمورا أمنية (القسم 23).
- المعلومات التي تحتويها سجلات المحكمة (القسم 32).
- حيثما يؤدي كشف المعلومات إلى انتهاك امتيازات برلمانية (القسم 34).
- المعلومات التي يحتفظ بها مجلس العموم أو مجلس اللوردات وحيث يتعارض كشف المعلومات مع المسار الفعال للشؤون العامة (القسم 36). (والمعلومات التي لا يتم الاحتفاظ بها في بمجلس العموم واللوردات والتي تندرج تحت القسم 36 تخضع لتقدير المصلحة العامة).
- المعلومات التي (أ) يمكن للمتقدم بطلب للحصول عليها وفقا لقانون حماية البيانات لسنة 1998، أو (ب) بكشفها سوف يتم انتهاك مبادئ حماية البيانات (القسم 40).
- المعلومات التي يتم تزويدها بمبدأ الثقة (القسم 41).
- عندما يكون محظورا الكشف عن المعلومات طبقا للقانون، أو عدم التوافق مع الالتزام بالوحدة الأوروبية أو سوف تتسبب في ازدراء للمحكمة (القسم 44).

الاستثناءات التقديرية Qualified Exemptions:

إذا أدرجت المعلومات ضمن الاستثناء التقديري، فإنه يجب أن تخضع لتقدير المصلحة العامة. وبذلك نجد أن القرار الصادر بشأن طلب كشف معلومات وفقا للاستثناء التقديري يخضع لمرحلتين، أولا على سلطة عامة أن تقرر ما إذا كان الاستثناء يغطي المعلومات أو لا، ثم حتى لو كانت المعلومات مشمولة بالاستثناء، فإن على السلطة أن تكشف المعلومات ما لم يشير طلب تقدير المصلحة العامة إلى أن المصلحة العامة تفضل عدم الكشف.

ويمكن تقسيم الاستثناءات التقديرية إلى فئتين:

- استثناءات قائمة على الفئوية والتي تغطي معلومات حول طبقات معينة .
- واستثناءات قائمة على الضرر، والتي تغطي موقف الكشف عن المعلومات فيه قد يتسبب في وقوع ضرر.

الاستثناءات القائمة على الفئوية Class - based Exemptions وفقا لهذا القانون:

- معلومات ينتوى نشرها في المستقبل (القسم 22).
- تستثنى المعلومات التي لا تندرج ضمن القسم 23(1) إذا ما تطلب الأمر ذلك لدواعي حماية الأمن القومي (القسم 24).
- المعلومات التي تجمعها السلطات العامة لأغراض التحريات والإجراءات (القسم 30).
- المعلومات المرتبطة بمعلومات حول سياسة الحكومة والاتصالات الوزارية ومشورة مستشاري الحكومة القانونيين وعمليات أي مكتب وزاري خاص (القسم 35).
- المعلومات التي ترتبط بالاتصالات بين أعضاء الأسرة المالكة (القسم 37).

- عمليات منع التداخل بين قانون حرية المعلومات واللوائح التي تتطلب الكشف عن معلومات بيئية (القسم 39).

- المعلومات التي يغطيها الامتياز القانوني المهني (القسم 42).

- الأسرار التجارية (القسم 43(1)).

الاستثناءات القائمة على الضرر والتي وردت في القانون Harm - based Exemptions:

وفقا لهذه الاستثناءات، من المحتمل أن يكون الاستثناء (الخاضع لتقدير المصلحة العامة) إذا ما كان ملتزما بالواجبات المندرجة تحت القسم الأول:

- يضر الدفاع أو القدرة والفعالية أو أمن أي من القوات المعنية (القسم 26).

- يضر بالعلاقات الدولية (القسم 27).

- يضر بالعلاقات بين أي من وزارات المملكة المتحدة وأي إدارة أخرى مناظرة (القسم 28).

- يضر بالمصالح الاقتصادية للمملكة المتحدة (القسم 29).

- يضر بتطبيق القانون (مثل منع الجريمة أو وزارة العدل،..إلخ) (القسم 31)

- يضر بوظائف تدقيق أي من السلطات العامة (القسم 33).

- ومن الرأي المناسب للشخص الذي يقوم بالتقدير: يضر بفعالية تنفيذ الشؤون العامة، أو يضر بالمسؤولية الجماعية أو يقيد مبدأ المشورة وتبادل وجهات النظر بحرية وصراحة (القسم 36).

- يعرض للخطر الصحة البدنية أو العقلية أو يعرض للخطر سلامة الأفراد (القسم 38).

- يضر بالمصالح التجارية (القسم 43(2)).

السلطة العامة ليست ملزمة بالموافقة على طلب معلومات إذا كان الطلب كيدي (القسم 14(1)).

ويعد الطلب كيديا إذا ما كان "استحواذي obsessive أو واضح عدم منطقيته"، يزعج السلطة أو يسبب الاكتئاب للعاملين أو يفرض عبئا ثقيلا أو إذا ما افتقر الطلب إلى أي قيمة جدية.

يؤثر القانون على 100.000 جهاز خدمة عامة بما في ذلك الإدارات الحكومية والمدارس والمجالس.

وقد جاء تنفيذ القانون على مراحل وانتهى تطبيقه في الأول من يناير 2005 "بالحق العام للدخول على المعلومات العامة" وفقا للقانون.

وإلى جانب "الحق العام للدخول على المعلومات"، يفرض القانون واجبا على السلطات العامة لأجل تطبيق والمحافظة على "خطط نشر" للكشف الروتيني عن المعلومات المهمة (مثل التقارير والحسابات السنوية). ويجب اعتماد خطط النشر هذه من قبل مفوض المعلومات.

وبشكل عام، للسلطات العامة 20 يوم عمل للاستجابة لطلب الحصول على معلومات برغم أنه بالإمكان مد هذا الوقت المحدد في حالات معينة و/أو بالاتفاق مع طالب المعلومات.

ووفقا للقانون، يتم تشجيع السلطات العامة على الدخول في حوار مع طالب المعلومات لحسن تقرير وتحديد المعلومات التي يطلبها والشكل التي يرغب أن ترد المعلومات عليه - في ذاتها، وهو ما يعد تغيير في الطريقة التي تتفاعل بها سلطات المملكة المتحدة مع الجمهور. ويمكن رفض الطلبات إذا

مـا كانـت تتكلـف مـا يزيـد عـن 600 جنيـه إسـترليني بمـا في ذلـك الوقـت المهـدر في عمليـة البحـث في الملفـات.

ولقـد أنشـأت حكومـة المملكـة المتحـدة "الدخـول عـلى الإدارة المركزيـة لتبـادل المعلومـات Access to Information Central Clearing House لأجـل التأكـد مـن توافـق تـداول طلبـات الحصـول عـلى المعلومـات مـن خـلال الحكومـة المركزيـة.

و بعـد هـذا العـرض نـري أن هنـاك ثلاثـة ملامـح لقانـون حريـة المعلومـات البريطـاني تسـتحق أن نوليهـا اهتمامـا خاصـا حيـث إنهـا تختلـف عـن موقـف كثـير مـن الـدول الأخـرى.

1. لمعظـم الأغـراض العمليـة، يتـم التعامـل مـع طلبـات الأفـراد للدخـول عـلى معلومـات الشـخصية مـن خـارج القانـون. إذ يتـم التعامـل معهـا وفقـا لقانـون حمايـة البيانـات لسـنة 1998 متـى تقـرر تطبيـق الاسـتثناء للبيانـات الشـخصية للطـرف الأول برغـم أن بعـض الأحـكام الرئيسـة تظـل في محـل التطبيـق مثـل حـق التقـدم بشـكوى إلى مفـوض المعلومـات.
2. يتـم التعامـل مـع طلبـات المعلومـات المعنيـة بأمـور تتعلـق بالبيئـة وفقـا للوائـح المعلومـات البيئيـة لسـنة 2004. وعـلى الرغـم مـن أن تلـك اللوائـح تتماثـل مـع قانـون حريـة المعلومـات فإنهـا تختلـف في عـدد مـن الطـرق.
3. ليـس هنـاك إجـراء يمكـن بموجبـه للأطـراف الأخـرى third parties أن تعـارض قـرار اتخذتـه سـلطة عامـة للكشـف عـن معلومـات: فعـلى سـبيل المثـال، إذا قدمـت هيئـة تجاريـة معلومـات لسـلطة عامـة وقامـت السـلطة العامـة بالكشـف عـن هـذه المعلومـات اسـتجابة للطلـب وفقـا لقانـون حريـة المعلومـات، ليـس للهيئـة التجاريـة الحـق في الاعـتراض

عـل ذلـك القـرار. وعـلى نقيـض حريـة المعلومـات، نجـد أن الطلبـات مـن هـذه النوعيـة شـائعة في الولايـات المتحـدة.

في الوقـت الـذي تـم فيـه تمريـر هـذا القانـون، كان المؤيـدون لتشريـع حريـة المعلومـات ينتقـدون مـشروع القانـون لتعقيده ولمـداه المحدود ولاحتوائـه على الاعتراض الـوزاري. ولقـد انتقـد اللـورد مـاكاي مـشروع القانـون في مجلـس اللوردات ووصفـه بأنه "غـير فعـال toothless" لاحتوائـه عـلى أحـكام تسـمح للـوزراء بالاعتراض عـلى الطلبات.

وعـلى النقيـض، كان رئيـس الـوزراء السـابق تـوني بلير مسـؤولا عن تمريـر القانون والـذي يعـد: "أحـد أكـبر أخطائـه في مسيرته المهنيـة". ويقـول بلـير: "بالنسـبة للقـادة السياسـيين، الأمـر مثـل أن تقـول لشـخص يضربـك عـلى رأسـك بعصـا، يـا هـذا، جـرب هـذه، وتناولـه مطرقـة. والمعلومـات لا يتـم السـعي إليهـا لأن الصحفـي شـغوف لمعرفتها أو لزيـادة معرفـة الأفـراد، وإنمـا تسـتخدم كسـلاح".

ولقـد انتقـد نظـيره مـن حـزب العـمال اسـتخدام الصحفيـين للقانون لأجـل القيام "بحمـلات اصطيـاد" للقصـص الداعـرة البذيئـة قائـلا: "قانـون حريـة المعلومـات ليـس للصحفيـين وإنمـا للنـاس.

وهـي في حاجـة إلي أن يتـم اسـتخدامها اسـتخداما جيـدا لأجـل تعزيـز الحكومـة الجيـدة. تحتـاج المعلومـات إلى أن يتـم تداولهـا بمسـؤولية وأنـا أؤمـن تمامـا أن هنـاك واجبـا ومسـؤولية عـلى عاتـق الإعـلام أيضـا."

وفي مقالـة حـول حريـة المعلومـات تحـت عنـوان "حمـل في زي ذئـب"، عـرض رودني أوسـتين الانتقـادات التاليـة لجوهـر القانـون:

- إن مـدى الاسـتثناءات أكـبر مـن أي مـن قوانـين حريـة المعلومـات المعمـول بهـا في دولـة ديمقراطيـة.
- الالتزامـات بوضـع خطـط للنـشر لهـا معـاني مائعـة تعنـى أنـه لـن يكـون هنـاك واجـب لنـشر معلومـات ذات طبيعـة متخصصـة.

- هناك اعتراض وزاري يقوض القانون. ولقد استخدم حق النقض والاعتراض خمس مرات: المرة الأولى لإيقاف نشر محاضر اجتماعات مجلس الوزراء المرتبطة بغزو العراق، المرة الثانية والثالثة استخدم من قبل الحكومات المتعاقبة لإيقاف نشر اجتماعات مجلس الوزراء المرتبطة بالمناقشات المتعلقة بأيلولة انتقال الملكية devolution. المرة الرابعة لإيقاف نشر سجل المخاطر حول إصلاح الخدمات الطبية القومية National Health Service في إنجلترا. والمرة الخامسة لإيقاف نشر الخطابات الخاصة للأمير تشارلز أمير ويلز والمرسلة إلى عدد من الوزارات الحكومية.

ولقد تم أيضا انتقاد التشريع لوجود "ثغرات" تسمح للسلطات بتجنب كشف معلومات حول مواقف معينة. فالشركات المملوكة لإحدى السلطات العامة تخضع عموما للقانون ولكن الشركات المملوكة لسلطتين أو أكثر من السلطات العامة ليست مشمولة في القانون.

الحقائق التي كشفها القانون Facts Revealed by the Act

تشمل الحقائق التي سلط القانون عليها الأضواء ما يلي:

- وافقت الحكومة على صرف مبلغ 1.5 مليون جنيه إسترليني لإنقاذ واحدة من أكثر المدارس المتعثرة في برامجها الأكاديمية الرائدة قبل الانتخابات العامة سنة 2005 بعشرة أيام.

- صرف الوزراء وأعضاء البرلمان آلاف الجنيهات على سيارات الأجرة كجزء من مصاريف الانتقال المقدرة 5.9 مليون جنيه إسترليني.

- تم توجيه اتهامات بالاغتصاب والتحرشات الجنسية وانتهاك حقوق الأطفال والقتل لدبلوماسيين أجانب ممن يحملون الحصانة الدبلوماسية أثناء عملهم في بريطانيا.

- لأربعة وسبعين ضابطا يخدمون في شرطة العاصمة سجلات جنائية.

- وجود برنامج تعذيب بريطاني سري في أعقاب الحرب مع ألمانيا، "في ذكرى معسكرات الاعتقال.

- دعمت المملكة المتحدة برنامج الأسلحة النووية الإسرائيلي ببيع إسرائيل 20 طنا من المياه الثقيلة في عام 1958.

- وفرت خدمات الصحة القومية زرع الإمبلانون (من موانع الحمل) للفتيات من عمر 13 سنة في محاولة لإيقاف عمليات الحمل في سن المراهقة.

كان (تعديل) مشروع قانون حرية المعلومات مشروع تقدم به أحد الأعضاء إلى مجلس العموم البريطاني في عام 2007 إلا إنه فشل في أن يتحول إلى قانون.

وكان عضو البرلمان المحافظ ديفيد ماكلين قد تقدم بمشروع القانون للتأكد من أن مراسلات أعضاء البرلمان مستثناة من قوانين حرية المعلومات. ولقد قال السير منزيس كامبيل من الحزب الديمقراطي الليبرالي أنه يجب ألا يكون هناك "قانون لأعضاء البرلمان وقانون مختلف لجميع الآخرين. ومع ذلك، فشل في تمرير القراءة الأولى للمشروع في مجلس اللوردات.

وإضافة إلى ذلك، قدم اللورد فالكونر تعليقات تقترح ببذل الوقت في تقرير ما إذا كان يجب تضمين المعلومات التي تندرج تحت بند الاستثناء في حد التكلفة المقدر ب 600 جنيه إسترليني أم لا.

ولقد جرت المشاورات حيث قالت الحكومة بأن التغيير سوف يخفض التكاليف ويحد من الطلبات على المعلومات العادية عديمة الأهمية، برغم أن النقاد قالوا إن الهدف من ذلك هو جعل المعلومات المحرجة في طي السرية.

المبحث الثالث

الجهود الدولية والإقليمية لحماية الخصوصية المعلوماتية

يثـار التسـاؤل هنا عن جهود المنظـمات والكيانات الدولية في:

- الحفـاظ عـلى البيانـات والمعلومـات فـما الـدور الذي لعبتـه منظمـة التعاون الاقتصـادي والتنميـة (**المطلـب الأول**).
- والاتحـاد الأوروبي(**المطلب الثاني**).
- ومـا هو دور الأمم المتحـدة (**المطلب الثالث**).

المطلب الأول

منظمة التعاون الاقتصادي والتنمية

Organization for Economic Co - operation and Development - OECD -

في حقل حماية الخصوصية المعلوماتية، فإن العديد من المنظمات الدولية طورت أنشطة مختلفة تهدف إلى تنظيم حماية المعلومات الخاصة، وتنظيم تدفق وانتقال البيانات، وقد أنجز الجزء الأكبر من هذا الجهد في هذا الحقل من قبل منظمة التعاون الاقتصادي والتنمية، ومجلس أوروبا، واتحاد أوروبا، والأمم المتحدة، ومجموعة الدول السبعة، ومنظمة التجارة العالمية.

منظمة التعاون الاقتصادي والتنمية: تضم منظمة التعاون الاقتصادي والتنمية في عضويتها 29 دولة[1] حتى أواخر عام 2000 وغرضها الرئيس تحقيق أعلى مستويات النمو الاقتصادي لأعضائها وتناغم التطور الاقتصادي مع التنمية الاجتماعية [2].

ابتداء من عام 1978 بدأت هذه المنظمة وضع أدلة وقواعد إرشادية بشأن حماية الخصوصية ونقل البيانات [3]، وقد تم تبني هذه القواعد من قبل مجلس المنظمة في عام 1980 مع التوصية للأعضاء بالالتزام بها، ولا تعد هذه القواعد إلزامية وإنما مجرد إرشادات وتوصيات، وتغطي هذه القواعد

---

(1) هذه الدول هي استراليا والنمسا وبلجيكيا وكندا وجمهورية التشيك والدنمارك وفنلندا وفرنسا وألمانيا واليونان وهنجاريا وأيسلندا وأيرلندا وإيطاليا واليابان وكوريا ولوكسمبورغ والمكسيك وهولندا ونيوزلندا والنرويج وبولندا والبرتغال وإسبانيا والسويد وسويسرا وتركيا وبريطانيا والولايات المتحدة الأمريكية.

(2) www.oecd.org

(3) OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980) p.53

الأشـخاص الطبيعيـين فقـط، وتطبـق عـلى القطاعـين العـام والخـاص، وتتعلـق أيضـا بالبيانـات المعالجـة آليـا أو غـير المعالجـة آليـا، وتتضمـن التوجيهـات المبـادئ الثمانيـة الرئيسـة لحمايـة الخصوصيـة أو الحـق في حمايـة البيانـات الخاصـة، وهـذه المبـادئ هـي:

- تحديـد حـصر عمليـات جمع البيانـات Collection - limitation والاقتصار عـلى طبيعـة البيانـات الشـخصية وتحديدهـا Data quality.
- تحديـد الغرض Purpose - specification.
- حصر الاسـتخدام بالغرض المحدد Use - limitation
- توفير وسـائل حمايـة وأمن المعلومات Security - Safeguards.
- العلانية Openness.
- الحق في المشاركة والمساءلة Individual Participation and Accountability.

ومثـل هـذا الدليـل الوثيقـة لعـب دورا رئيسـا وكان الأكـثر تأثـيرا في اتجـاه الدول الأوروبيـة إلى إقـرار تشريعـات وطنيـة في حقـل الخصوصيـة، ومنـذ ذلـك التاريـخ تتابـع هـذه المنظمـة موضـوع الخصوصيـة وتضعـه ضمـن أجندتهـا السـنوية وتتابـع تطـورات التدابـير التشريعيـة في هـذه الحقـل.[1]

---

(1) The Organization for Economic Co - Operation and Development، "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data"، available at http://www.oecd.org/document /180،2340/،en_2649_34255_1815186_1_1_1_1،00.html (last modified January 5، 1999) P.21

المطلب الثاني

مجلس أوروبا Council of Europe

تحقق وجود اتفاق عالمي بشأن حماية الخصوصية عن طريق مجلس أوروبا الذي هو بالأصل معني بحقوق الإنسان، وذلك بوضع الاتفاقية الأوروبية لحقوق الإنسان والحريات العامة لعام 1950 حيث أوجبت المادة الثامنة من هذه الاتفاقية - المتقدم الإشارة إليها - حماية الحياة الخاصة بالنص على وجوب حماية الأفراد من التدخل والاعتداء على حياتهم الخاصة وحياة أسرهم، كما قررت المادة العاشرة من هذه الاتفاقية وجوب حماية حق الوصول إلى المعلومات..[1]

صُممت المقترحات الأوروبية الجديدةخصيصا لتعزيز سلطة الجهات المدافعة عن حماية المعطيات الشخصية، والمراقبة للجهات التي ترتكب خللا في هذا المجال. وتطالب هذه المقترحات الشركات بإخطار الجهات التنظيمية في حالة تمت سرقة البيانات أو أسيء استغلالها.[2]

تمنح هذه المقترحات البلدان الأعضاء في الاتحاد الأوروبي سلطات جديدة تمكنها من فرض غرامات تتجاوز 1% من مجموع إيراداتها في حالة انتهاك قواعد الاتحاد بشأن حماية البيانات الشخصية.

تضمن هذه المقترحاتللأفراد المزيد من الحقوق، بما في ذلك "الحق في النسيان"، وهو الذي يسمح للأفراد بالمطالبة بإلغاء بياناتهم وعدم الاحتفاظ بها إلكترونيا..

(1) K،Kevien،M. "New draft European data protection regime". law group،(2003) p.46

(2) Asscher، L، Hoogcarspel، S.A، Regulating Spam: A European Perspective after the Adoption of the E - Privacy Directive (T.M.C. Asser Press 2006) P 56

تنشئ هذه القواعد الجديدة "الحق في نقل البيانات" للتأكّد من أن الأفراد يمكن لهم بسهولة نقل معلوماتهم الشخصية بين مختلف الشركات أو الخدمات.

تأتي هذه القواعد الجديدةفي ظل توسع نطاق الكيفية التي يستخدم بها الناس الإنترنت اليوم. فشبكات التواصل الاجتماعي، مثل فيسبوك ولينكدين وغوغل، بلغ عدد أعضائها مليار مستخدم، في حين أن ما يسمى خدمات الحوسبة الرئيسة، والتي تسمح للشركات وللأفراد بتخزين البيانات على خوادم بعيدة تسمح بالوصول إليها أيْنما كانت سوف تصبح الاتجاه السائد.

قبل الشروع في تنفيذها، تحتاج القواعد المقترحة من طرف الاتحاد الأوروبي إلى موافقة البلدان الأعضاء، ومن المحتمل أن يستغرق ذلك سنتيْن على أقل تقدير، وأن تتغيّر تلك القواعد إلى ذلك الحين، ولذلك ليس من المنتظر مطالبة شركات خدمات الإنترنت باحترامها وتنفيذها قبل عام2014 وربما 2015.[1]

مجلس أوروبا [2]Council of Europe:

تحقق وجود اتفاق عالمي بشأن حماية الخصوصية عن طريق مجلس

---

(1) http://www.swissinfo.ch/ara/detail/content.html visited 6 - 2013

(2) The Council of Europe is the continent's leading human rights organisation. It includes 47 member states، 28 of which are members of the European Union. All Council of Europe member states have signed up to the European Convention on Human Rights، a treaty designed to protect human rights، democracy and the rule of law. The European Court of Human Rights oversees the implementation of the Convention in the member states. Individuals can bring complaints of human rights violations to the Strasbourg Court once all possibilities of appeal have been exhausted in the member state concerned. The European Union is preparing to sign the European Convention on Human Rights، creating a common European legal space for over 820 million citizens.

أوروبا الذي هو بالأصل معني بحقوق الإنسان، وذلك بوضع الاتفاقية الأوروبية لحقوق الإنسان والحريات العامة لعام 1950 حيث أوجبت المادة الثامنة من هذه الاتفاقية - المتقدم الإشارة إليها - حماية الحياة الخاصة بالنص على وجوب حماية الأفراد من التدخل والاعتداء على حياتهم الخاصة وحياة أسرهم، كما قررت المادة العاشرة من هذه الاتفاقية وجوب حماية حق الوصول إلى المعلومات.

في عام 1981 تبنت لجنة وزراء من مجلس أوروبا أنيط بها معالجة موضوع الخصوصية اتفاقية حماية الأفراد في نطاق المعالجة الآلية للبيانات الشخصية (Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data) وقد وقعت على هذه الاتفاقية 31 دولة صادق منها 21 دولة ولا تزال عشرة دول غير مصادقة وفقا لواقع الاتفاقية بتاريخ 2000/1/31 وقد أصبحت هذه الاتفاقية نافذة بتاريخ 1985/10/1.

وعلى خلاف توصيات منظمة التعاون الاقتصادي والتنمية، فإن هذه الاتفاقية ملزمة للأعضاء المتعاقدين وينحصر نطاقها بالأشخاص الطبيعيين وبالملفات المؤتمتة، وتطبق على الملفات المؤتمتة في القطاعين العام والخاص، وتقرر هذه الاتفاقية عشر مبادئ تمثل الحد الأدنى لمعايير حماية الخصوصية المتعين على الدول الأعضاء تضمينها في التدابير التشريعية والقوانين التي تضعها، وهذه المبادئ مقاربة جدا لمبادئ منظمة التعاون الاقتصادي والتنمية ولكن مع مزيد من التفصيلات وهي: (تحقيق العدل الاجتماعي، قيود الجمع، الوقاية، العلنية، توقيت الغرض وتحديد المدى، الدقة، مشاركة الأفراد) واستناد إلى هذه المبادئ الأساسية للحماية فإن قواعد الاتفاقية تغطي مسائل نقل وتبادل البيانات بين الدول المتعاقدة وتمنع نقل أية معلومات خارج الحدود إلا للدولة التي تتوفر لها حماية موازية مع استثناءات مع هذه القاعدة.

وقد بذل مجلس أوروبا جهودا إضافة في هذا الحقل من خلال لجنة

الخبراء العاملة في حقل حماية المعطيات، وقد أصدرت هذه اللجنة سلسلة من الأدلة التوجيهية المعتمدة على الاتفاقية المذكورة وهي ليست أكثر من توصيات موجهة إلى حكومات دول الأعضاء وتتعلق توصيات اللجنة بحماية قواعد المعلومات الطبية المؤتمتة وقواعد المعلومات الخاصة المتعلقة بالأنشطة الطبية والإحصاءات وقواعد المعلومات الخاصة لأغراض التسويق وقواعد المعلومات الخاصة لأغراض الضمان الاجتماعي وكذلك لأغراض البوليس والبيانات الجنائية وقواعد المعلومات الخاصة بأغراض التوظيف وكذلك خدمات الاتصال، وقد عمل جزء من اللجنة المذكورة على موضوع البيانات المتعلقة بالقطاع المصرفي وتحديدا البيانات الخاصة بالبطاقات الماهرة ونقل البيانات من نقاط البيع (مخارج البيع)[1]

و يلاحظ أن جهود مجلس أوروبا في حقل حماية البيانات تعد أقل من الجهود الذي يقوم بها الاتحاد الأوروبي حيث أصدر الأخير التوجيه الأوروبي الخاص بحماية البيانات الشخصية والذي يعد دليلا في مسألة حماية البيانات الشخصية في العصر التكنولوجي.

(1) William J. Clinton & Albert Gore، Jr.، "A Framework for Global Electronic Commerce"، (July 1، 1997) P.146

المطلب الثالث

الأمم المتحدة United Nation

الأمـم المتحدة United Nation

في عـام 1989 تبنـت الأمـم المتحـدة دليـلا يتعلـق باسـتخدام الحوسـبة في عمليـة تدفـق البيانـات الشـخصية، وبتاريـخ 90/12/14 تبنـت الهيئـة العامـة دليـل تنظيـم اسـتخدام المعالجـة الآليـة للبيانـات الشـخصية[1]، ويتضمـن هـذا الدليـل المبـادئ ذاتهـا المقـررة لـدى منظمـة التعـاون الاقتصـادي والتنميـة ولـدى مجلـس أوروبـا والاتفاقيـات المشـار إليهـا أعـلاه، وهـي مبادئ غـير ملزمـة ومجرد توصيـات للـدول الأعضـاء لتضمينها التدابـير التشريعيـة في هـذا الحقـل وقـد بذلـت العديد مـن الجهـود لحمايـة الخصوصية مـن قبـل لجنـة حقـوق الإنسـان في المجلـس الاقتصـادي والاجتماعـي في الأمـم المتحـدة.

وقـد صوتـت الأمـم المتحـدة (UN) بالإجـماع في السـادس والعشريـن مـن نوفمبر 2013علـى تبنـي قـرار يدعـو الخصوصيـة عـلى شـبكة الإنترنـت لتكـون معـترف بهـا كحق مـن حقوق الإنسـان.[2]

هـذا القـرار يمتـد حـق الإنسـان عامـة مـن الخصوصيـة إلى عـالم الإنترنـت ويأخـذ بوضـوح تهـدف إلى الولايـات المتحـدة الأمريكيـة لأنشـطتها كشـفت مؤخـرا في البنـد 4، والـذي "يدعـو جميـع الـدول" إلى تنفيـذ الإجـراءات التاليـة:

---

(1) Prof. Dr. Ulrich Sieber، "Legal Aspects of Computer - Related Crime in the Information Society "(COMCRIME Study) (Jan. 1، 1998(p.145

(2) THIRD COMMITTEE APPROVES TEXT TITLED 'RIGHT TO PRIVACY IN THE DIGITAL AGE'، https://www.un.org/News/Press/docs/2013/gashc4094.doc.ht retrived 152014/6/

(أ) احترام وحماية الحق في الخصوصية، بما في ذلك في سياق الاتصالات الرقمية.

(ب) اتخاذ تدابير لوضع حد لانتهاكات هذه الحقوق وتهيئة الظروف لمنع هذه الانتهاكات، بما في ذلك من خلال ضمان التشريعات الوطنية ذات الصلة مع التزاماتها بموجب القانون الدولي لحقوق الإنسان.

(ج) أن تعيد النظر في الإجراءات والممارسات والتشريعات المتعلقة بمراقبة الاتصالات، واعتراض وجمع البيانات الشخصية، بما في ذلك المراقبة الشاملة، اعتراض، وجمع، وذلك بهدف الحفاظ على الحق في الخصوصية من خلال ضمان التنفيذ الكامل والفعال للجميع التزاماتها بموجب القانون الدولي لحقوق الإنسان.

(د) إنشاء أو الحفاظ على الآليات القائمة مستقلة وفعالة المحلي الرقابة قادرة على ضمان الشفافية، حسب الاقتضاء، والمساءلة عن مراقبة الدولة من الاتصالات، واعتراض وجمع البيانات الشخصية؛[1]

و يري الباحث أن الأمم المتحدة قد أقرت صراحة الحقوق نفسها التي لدى الناس حاليا يجب أن تكون محمية عبر الإنترنت، بما في ذلك الحق في الخصوصية حيث إن الطابع العالمي للإنترنت أدى إلى الانفتاح والتقدم السريع في تكنولوجيا المعلومات والاتصالات تكنولوجيات كقوة دافعة في تسريع التقدم نحو تحقيق التنمية بمختلف أشكالها وعلى الرغم من ذلك فإن مثل هذه القرارات والتوجيهات الصادرة عن الأمم المتحدة ليست ملزمة ويمكن مخالفتها.

(1) THIRD COMMITTEE APPROVES TEXT TITLED 'RIGHT TO PRIVACY IN THE DIGITAL AGE'، https://www.un.org/News/Press/docs/2013/gashc4094.doc.ht retrived 152014/6/

الباب الثاني

حماية البيانات الشخصية المتداولة عبر الإنترنت

تمهيد وتقسيم:

أصبحت البيانات والمعلومات الشخصية في ظل العصر الرقمي متاحة وفي أغلب الأحيان غير مؤمنة، وهنا يثار التساؤل عن:

- أنواع المخاطر التي تهدد خصوصية البيانات الشخصية عبر شبكة الإنترنت **(الفصل الأول)**.
- و بالإضافة إلى التساؤل عن كيفية حماية خصوصية البيانات المتداولة عبر الإنترنت من الناحية الجنائية **(الفصل الثاني)**.

الفصل الأول

المخاطر التي تهدد خصوصية البيانات الشخصية المتداولة عبر شبكة الإنترنت

تتعدد المصادر التي تهدد خصوصية البيانات الشخصية وهنا يجب الإجابة عن التساؤل عن:

- أثر تقنية المعلومات على خصوصية البيانات (**المبحث الأول**).
- وكذلك أثر العقود الإلكترونية التي تفرض التخلي الطوعي عن البيانات (**المبحث الثاني**).
- وما الإطار الأساس لحماية البيانات الشخصية المعترف بها (**المبحث الثالث**).

المبحث الأول

أثر تقنية المعلومات على حماية الحياة الخاصة

لقد أثر التطور الهائل في مجال تكنولوجيا المعلومات على حرمة البيانات الشخصية وهنا يثار التساؤل عن:

- مدي تأثير التطور التقني على خصوصية البيانات **(المطلب الأول)**.
- وكذلك تحديات حماية خصوصية البيانات عبر شبكة الإنترنت **(المطلب الثاني)**.
- وما مصادر تهديد خصوصية البيانات عبر شبة الإنترنت **(المطلب الثالث)**.
- وما التناقضات التي تثار في مجال الكشف عن البيانات والاستفادة من إعلانها**(المطلب الرابع)**.

المطلب الأول

خصوصية البيانات في ظل تطور تكنولوجيا المعلومات

أصبحت خصوصية البيانات (أو المعلومات) إحدى حقول البحث متزايدة الأهمية في عصرنا الحالي -عصر تقنية المعلومات، خاصة في إدارة بيانات المؤسسات والإدارات الحكومية وكذلك الشركات الخاصة التجارية والخدمية والصحية، تلك التي تقوم بتخزين مئات الآلاف أو الملايين من سجلات العملاء أو المواطنين، والتي تتضمن بياناتهم الشخصية واهتماماتهم، والأنشطة التي قاموا بها وميولهم، مع الإمكانية الجبارة في تحليل هذه البيانات ومقارنتها وسهولة نقلها بين القارات في ثوان معدودة.

وبتصاعد عدد المخترقين (Hackers) وسارقي الهويات (Identity Theft)، فعمليات اختراق خصوصية البيانات تقوم بالتأثير على حياتنا الخاصة وأعمالنا بشكل لم نكن لنتخيله من قبل. والأرقام تتحدث، فوفقاً لتقرير منظمة (Privacy Rights Clearinghouse - PRC)، أنه منذ شهر يناير 2005 إلى سبتمبر 2008، [1]فإن عدد السجلات التي تحتوي على معلومات شخصية حساسة وتم اختراقها أمنياً في الولايات المتحدة فقط تجاوزت 230،411،730 سجل، والعدد في ازدياد يومي.

إن الخصوصية، وبصفة عامة، هي مقياس غير موضوعي، أي يختلف تعريفها وحدودها من بيئة إلى أخرى. ولكن الصفة المشتركة في جميع هذه التعريفات هي منظور أن الخصوصية إحدى حقوق الإنسان في حياته، ولكنها تعتمد بشكل أساسي على البيئة والسياق. [2]

---

(1) The report available at https://www.privacyrights.org/speeches - testimony

(2) Roger Clarke's Privacy and Social Media: An Analytical Framework، "Data Surveillance and Information Privacy" (2013) p.126

قـام روجـر كلارك، الاستشـاري والخبـير في خصوصيـة البيانـات والأعـمال الإلكترونيـة، بتعريـف الخصوصيـة بأنهـا: "قـدرة الأشـخاص عـلى المحافظـة عـلى 'مسـاحتهم الشـخصية'، في مأمـن مـن التدخـل مـن قِبـل منشـآت أو أشـخاص آخريـن"، وقـام بتحديـد مسـتويات (أبعـاد) مـن الخصوصيـة، منهـا مـا يتعلـق بمحـل البحـث هنـا:[1]

1. **خصوصية الاتصالات الشخصية: (Privacy of personal communications)[2]:**

وهـي مطالبـة الأشـخاص بالقـدرة عـلى الاتصـال فيـما بينهـم دون المراقبـة الروتينيـة مـن قِبـل أشـخاص آخريـن أو منظـمات، وهو ما يشـار إليـه أحياناً "باعـتراض الخصوصيـة" (Privacy Deception).

2. **خصوصيــة البيانــات الشــخصية (Privacy of personal Data)[3]:**

وهــي مطالبــة الأشــخاص بــأن لا تكــون البيانــات الخاصــة عنهــم متوفــرة تلقائيــاً لغيرهــم مــن الأفــراد أو المنظــمات،

---

(1) Roger Clarke's The Nature of the Digital Persona and Its Implications for Data Protection Law (January، for Bahcesehir Uni، Istanbul (2014) p.78

(2) privacy of personal communications. Individuals claim an interest in being able to communicate among themselves، using various media، without routine monitoring of their communications by other persons or organisations. This includes what is sometimes referred to as ‹interception privacy›

(3) privacy of personal data. Individuals claim that data about themselves should not be automatically available to other individuals and organisations، and that، even where data is possessed by another party، the individual must be able to exercise a substantial degree of control over that data and its use. This is sometimes referred to as ‹data privacy› and ‹information privacy›

حتـى في حالـة أن تكـون البيانـات مملوكـة مـن طـرف آخـر، فلهـم القدرة علـى ممارسـة قـدر كبـير مـن السـيطرة أو التحكم بتلـك البيانـات وطريقة اسـتخدامها. وهـذا مـا يعـرف " بخصوصيـة المعلومـات أو خصوصيـة البيانـات". وعرّفهـا روجـر بأنهـا: "رغبـة الشـخص بالتحكـم، أو عـلى الأقـل التأثـير بشـكل كبـير في كيفيـة التعامـل مـع بياناتـه الشـخصية".

اسـتخلص باحثـان مـن جامعـة تكسـاس في أوسـتن، إمكانيـة اكتشـاف هويـة المسـتخدمين مجهـولي الهويـة في الشـبكة الاجتماعيـة المعروفة عالميـا "تويتر" (Twitter)، والمسـجلين أيضـاً في شـبكات اجتماعيـة أخـرى، وذلـك بمراقبـة شـبكة اتصـالات هـؤلاء المسـتخدمين مـع الشـبكات الأخـرى.

وقـد ذكـر الباحثان[1]:"لقـد قمنـا بتقديـم دليـل ملمـوس عـلى نجـاح عمـل الخوارزميـة (De - Anonymization Algorithm) وذلـك مـن خـلال تجربتهـا عـلى أشـهر شـبكتين اجتماعيتـين في الإنترنـت ’تويـتر’ و’فليكـر’، وتبين لنـا أن ثلث المسـتخدمين المجهـولي الهويـة، أعضـاء عشـوائيين، في الشـبكتين يمكـن اكتشـافهم، أي إعـادة تعريـف هويتهـم، مـن خـلال الرسـم البيـاني لشـبكة ’تويـتر’، بوجـود نسـبة خطـأ 12% فقـط، مع الرغـم بـأن نسـبة التداخـل بـين هـؤلاء الأعضـاء هـي أقـل مـن 15%".

النتيجـة هـي أن محاولـة البقـاء متخفيـاً في الشـبكات الاجتماعيـة بالدخـول بأسـماء مختلفـة أو بإدخـال بيانـات غـير صحيحـة أمـر يمكـن اكتشـافه ويمكـن تكويـن صـورة عـن المسـتخدم واهتماماتـه، وذلـك باسـتخدام خوارزميـات التقنيـات الحديثـة، مـن تنقيـب البيانـات (Data Mining) ودراسـة السـلوكيات وغيرهـا.

---

(1) Arvind Narayanan and Vitaly Shmatikov،De - anonymizing Social Networks،The University of Texas at Austin،(2012) p.171

مسجل نقرات لوحة المفاتيح (أو KeyLogger)، هي برامج أو أجهزة مراقبة، لها إمكانية تسجيل النقرات على لوحة المفاتيح والتقاط صور لشاشات العرض والقيام بتخزينها في ملفات التسجيل (Log files)، مع إمكانية التوثيق لهذه البيانات، من دون علم المستخدم.

قد تستخدم هذه الأداة في سرقة البيانات الشخصية كبيانات البطاقات الائتمانية وكلمات المرور والرسائل البريدية وعناوين الصفحات الإلكترونية وغيرها. وفي الجانب الآخر من الاستخدام، فقد تستخدم هذه الأداة لمراقبة الأجهزة الخاصة، إن تم استخدامها من قِبل أشخاص غير مصرح لهم، وقد تقوم بعض الشركات بمراقبة بعض الموظفين للتأكد من عدم إرسالهم لبيانات خاصة بالمنشأة إلى المنافسين أو بيعها لأغراض خاصة.

نستنتج من المثالين السابقين أن تطبيقات تقنية المعلومات سلاح ذو حدين، والمستخدم هو من يقرر أي الحدين يستخدم، فمثلاً خوارزمية ال (De - Anonymization) إن تم استخدامها في التعرف على الأشخاص المشبوهين في التخطيط لعمليات إرهابية أو الترويج للمخدرات أو المواد الإباحية، فعندها قد استخدمنا هذه التقنية لصالحنا وصالح الأمة، أما إن استخدمت لأمور الابتزاز أو التعدي، فعندها أصبحنا كمن نقضت غزلها من بعد قوة.

إن من أكثر التحديات صعوبة في إدارة أمن البيانات الخصوصية هي الامتثال للأنظمة، حيث قامت مؤخراً -في نوفمبر 2008 - مؤسسة أ.م.ر للبحوث [1](AMR Research Ltd.) باستطلاع شمل 154 متخذ قرار في كبرى شركات تقنية المعلومات في الولايات المتحدة الأمريكية.

استخلص البحث أن أكثر ثلاث صعوبات في إدارة خصوصية البيانات هي: تعدد واختلاف سياسات الخصوصية في المناطق المختلفة -جغرافياً،

---

(1) http://www.gartner.com/technology/supply - chain - professionals.jsp

ومواكبة التغييرات المستمرة في الأنظمة والسياسات، وأخيراً إجبار الأفراد والمنشآت الحكومية لاتباع هذه القوانين والأنظمة.

واستُنتِج أيضاً، بأن أكثر ما يخشى عليه أصحاب الشركات في قضايا خصوصية البيانات هي خسارة ثقة العملاء والموظفين والمستثمرين والعلامات التجارية، ثم يأتي خشية فقدان الحقوق الفكرية للمنتجات والبحوث والدراسات، ومن ثم يأتي الخوف من التلاعب بالحسابات المالية للمنشأة.

والجدير بالذكر أن 55% من الشركات المشاركة في الاستطلاع ستقوم بزيادة قيمة الاستثمار الداخلي في قضايا حفظ خصوصية البيانات في عام 2009 مقارنة بما أنفقته في العام الأسبق، وتتمثل هذه الزيادة باستخدام التقنيات والسياسات الحديثة مثل: أمن الشبكات (من جدران نارية ومضادات الفيروسات والشبكات الخاصة الافتراضية)، وأدوات مراقبة أنشطة قواعد البيانات، والأمن الاحترازي (من أنظمة كشف التلاعب وكشف نقاط ضعف التطبيقات والشبكات)، وغيرها من الأنظمة والأدوات التي تساعد المنشآت في حماية خصوصية بياناتها.

يقول جيري بيرن Jerry Berman وديردري موليغان Deirdre Mulligan، "تصور أنك تسير في أحد مخازن الأسواق بين مخازن عديدة لا تعرف أيا منها، فتوضع على ظهرك إشارة تبين كل محل زرته وما الذي قمت به وما اشتريته، إن هذا شيء شبيه لما يمكن أن يحصل في بيئة الإنترنت " [(1)]

عندما يستخدم الأفراد مواقع الإنترنت فإنهم يتوقعون قدرا من الخفية في نشاطهم أكثر مما يتوقعون في العالم المادي الواقعي، ففي الأخير يمكن ملاحظة وجودهم ومراقبتهم من قبل الآخرين، وما لم يكشف الشخص عن

---

(1) Jerry Berman & Deirdre Mulligan، Privacy in the Digital Age: Work in Progress، Nova Law Review، Volume 23، Number 2، The Internet and Law، (Winter 1999) P.4

بيانـات تخصـه فإنـه يعتقـد أن أحـدا لـن يعـرف مـن هـو أو مـاذا يفعـل، لكـن الإنترنت عـبر نظـم الخـوادم ونظـم إدارة الشـبكات تصنـع قـدرا كبـيرا مـن المعلومـات عنـد كل وقفـة في فضـاء الشـبكة. وهـذه البيانـات قـد يتـم اصطيادهـا ومعرفتهـا عـن موظفـي منشـاة مـا – مثلا - مـن قبـل صاحـب العمـل عنـد اسـتخدامه للشـبكة أو لاشـتراكاتهم المربوطـة عليهـا، وقـد تجمـع مـن قبـل المواقـع المـزارة نفسـها، وكـما قلنـا فـإن جمـع شـتات معلومـات وسـلوكيات معينـة قـد يقـدم أوضـح صـورة عـن شـخص لم يـرد كشـف أيـا مـن تفاصيـل مـا تضمنتـه

ونظـرا لعـدم توفـر القـدر الـكافي مـن الحمايـة القانونية عـبر شـبكة الإنترنت فإن المعلومـات المعلنـة مـن قبـل الأفـراد تكـون بمثابـة التنـازل الضمنـي عـن تلـك المعلومات هـذا لا يمنـع وجـود وسـائل الحمايـة مثـل رسـائل التأكيـد وسياسـات الخصوصيـة، ولكـن هـذه الضمانـات لا توفـر القـدر الـكافي مـن حمايـة خصوصيـة البيانـات المعلـن عنها.[1]

وقـد أتاحـت التكنولوجيـا وتقنيـه المعلومـات قـدرا هائـلا مـن المرونـة وسـهولة الحصـول عـلى المعلومـات وهـذا يعـد سـلاحا ذا حديـن فسـهوله الوصـول لبيانـات وإمكانيـة معالجتهـا والاسـتفادة منهـا عـلى جانـب، ومـن ناحيـة أخـري عـدم توفـير الحمايـة اللازمـة لخصوصيـة تلـك المعلومـات وعـلى ذلـك فيجـب الموازنـة بين الاسـتفادة مـن الإفصـاح عـن البيانـات وتوفـير الحمايـة اللازمـة لهـا.

فالتطـور التكنولوجـي أصبـح يمكـن مـن جمـع أنـواع جديـدة مـن المعلومـات الشـخصية - فقـد نتـج عـن التقـدم التكنولوجـي ابتـكار أدوات لجمـع وفهـم أنـواع مختلفـة مـن المعلومـات كان يسـتحيل أو مـن غـير الممكـن الوصـول إليهـا في المـاضي.

فقـد يسـهل عمليـه جمـع المعلومـات الشـخصية وتحديـد مواقعهـا - يختـص

---

(1) Hunton & Williams LLP، New Requirements for Online Privacy Policie،Basic Books 2004 P 21).

كل جهاز كمبيوتر أو هاتف نقال أو أي جهاز آخر متصل بالإنترنت بعنوان بروتوكول إنترنت IP فريد يوفر محدد هوية فريد لكل جهاز، وهو ما يعني أنه يمكن تتبع هذه الأجهزة، فالقدرة على تحديد موقع أي جهاز من الأجهزة نشأ عنها تحديات كبيرة وجديدة بشأن الخصوصية، ويهيئ قدرات جديدة للحكومة والقطاع الخاص لتحليل المعلومات الشخصية فالقوة الحاسوبية الزائدة تعني أنه يمكن بدون تكلفة وبشكل فعال تخزين كميات هائلة من المعلومات ودمجها وتحليلها بمجرد جمعها، ويسمح التقدم التكنولوجي بالربط بين قواعد بيانات المعلومات مع بعضها البعض، الأمر الذي يتيح المزيد والمزيد من كميات البيانات التي يمكن معالجتها، كذلك يهيئ فرصاً جديدة للاستخدام التجاري للبيانات الشخصية حيث إن الكثير من الخدمات التي تقدمها هذه الشركات هي خدمات مجانية وتعتمد نماذج أعمالها على جمع معلومات المستخدم واستخدامها في أغراض التسويق.[1]

وقد بدأ الوصول إلى الإنترنت في الاتساع بشكل سريع عبر معظم دول العالم، إذ تشير الإحصاءات الواردة من الاتحاد الدولي للاتصالات السلكية واللاسلكية[2]، إلى أنه بين العام 2005 و2010 فقط، تضاعف عدد المستخدمين للإنترنت، ففي العام 1995 فقط 0،4 بالمائة من سكان العالم كانوا يستخدمون الإنترنت، وبحلول شهر مارس 2011 ارتفعت هذه النسبة حتى وصلت إلى 30،2 بالمائة وهو ما يعادل أكثر من ملياري مستخدم للإنترنت، 1.2 مليار منهم في الدول المتقدمة[3]، كما كان استخدام الهواتف النقالة أكثر ارتفاعاً بكثير.[4]

---

(1) Eneken Tikk،IP addresses subject to Personal data regulation،Out Law، 2013 P34

(2) ITU (International Telecommunication Union) is the United Nations specialized agency for information and communication technologies – ICTs.

(3) دراسة استقصائية عالمية حول خصوصية الإنترنت وحرية التعبير، سلسلة اليونسكو بشأن حرية الإنترنت 2013/11/28 ص102

(4) ICT report،THE WORLD IN 2010، The rise of 3G، ICT Figers and Facts،2010 P 1 - 10

و مـن هنـا نخلـص إلى أن كلـما زاد التطـور التقنـي والإبـداع الفنـي في مجـال التكنولوجيـا زادت المخاطـر التـي تهـدد خصوصيـة البيانـات الشـخصية إذ تسـتطيع الأنظمـة التـي تتسـلل عـلى أجهـزة الحاسـب الآلي والهواتـف الذكيـة - بمجـرد الدخـول عـلى شـبكة الإنترنـت - أن تنقـل جميـع البيانـات والمعلومـات المسـجلة عـلى الجهـاز وبـدون تصريـح معلـن لتكويـن قواعـد بيانـات ثـم الاتجـار بهـا فيـما بعـد.

المطلب الثاني

تحديات حماية خصوصية البيانات الشخصية عبر الإنترنت

إن وضع نظام لحماية الخصوصية في بيئة الإنترنت عليه أن يراعي طبيعة التهديدات الخاصة التي تتعرض لها الخصوصية في نطاق استخدام شبكة الإنترنت، فالإنترنت تخلق سلسلة من التحديات الجديدة في مواجهة خطط حماية المستهلك والطفولة وحماية الخصوصية.

- وتتمثل هذه التحديات في أن الإنترنت تزيد من كمية البيانات المجمعة والمعالجة والمنشأة (**الفرع الأول**).
- فهنا تثار تحديات السيطرة على البيانات المتدفقة عبر الإنترنت حيث إنها تتيح تدفق المعلومات (**الفرع الثاني**).
- مع عدم القدرة على السيطرة على ذلك التدفق نتيجة اللامركزية (**الفرع الثالث**).

الفرع الأول

الإنترنت يزيد كمية البيانات المجمعة والمعالجة والمنشأة

إن الإنترنت شهد نماء التوجه نحو جمع البيانات المتوفرة في العالم الحقيقي باعتبارها تصبح أكثر سهولة في بيئة الإنترنت من حيث قدرة الوصول إليها، وأكثر ملائمة للتبويب بسبب تقنيات الحوسبة، وتصبح أسهل للتبادل في ضوء وسائل تبادل المعلومات بكل أشكالها التي أتاحها الإنترنت وبرمجيات التصفح والتبادل والنقل.

فالبيئة التي تمر عبرها رحلة البيانات المتبادلة تغيرت بسبب الإنترنت، وترك الأفراد خلفهم الوسائل التقليدية في الوصول للمعلومات، وأصبح اعتمادهم أكثر فأكثر على الإنترنت، لأن الإنترنت مصدر غني بالمعلومات حول كل شيء، وفي نطاق مسائل الخصوصية تحديدا فإن المعلومات عن الأفراد وعاداتهم وهواياتهم وسلوكياتهم وآرائهم واتجاهاتهم في التسوق أمست متوفرة في ظل الإنترنت. [1]

إن البيانات المنقولة والمتبادلة والتي يطلق عليها تعبيرات عديدة كنهر المعلومات المتدفق كناية عن دور الفأرة من بين أدوات جهاز الكمبيوتر في عمليات تنزيل قدر كبير من المعلومات، قد تشمل عنوان بروتوكول الإنترنت لحواسيب الأفراد، المتصفح المستخدم، نوع الحاسوب، وآخر ما قام به المستخدم في زيارته الأخيرة السابقة لزيارة الموقع وربما المواقع الأخرى التي زارها، فهذه المعلومات التي قد تكون كافية أو لا تكون كذلك للتعريف بالشخص يتم اصطيادها وجمعها في نقاط عديدة في الرحلة عبر الشبكات، ويمكن أن تتوفر لإعادة استخدامها أو إفشائها أو تناقلها بين قطاعات معنية بجمعها، وبعض المعلومات مهمة وضرورية لعمليات الشبكة والوصول

(1) عبد الحميد بسيوني،الحماية من أخطار الإنترنت، دار الكتب العلمية،2003 ص 159.

لمواقع الإنترنت، كرقم التليفون وعنوان بروتوكول الإنترنت الخاص، وبدونهما فالشبكة غير قادرة على العمل، ولكن هناك أجزاء من المعلومات قد لا تكون ضرورية لهذه العمليات وقد يكون جمعها لأغراض غير عمليات الشبكة، ومع المعلومات التي تجمع في مراحل شراء المنتجات أو لمجرد التسجيل أو الاشتراك بخدمات الموقع، فإن جماع هذه المعلومات قد يشكل بيانا بأنشطة الفرد، وفي مرحلة من المراحل تصبح هذه البيانات عند جمع شتاتها وتحليلها، خاصة مع قيام برمجيات ذكية بذلك مادة تكشف تفاصيل كثيرة قد لا يرغب الشخص بكشفها، وفي الوقت نفسه تصبح هذه البيانات مادة غنية ومحلا للبيع من جهة لأخرى لغايات الأعمال والأنشطة.[1]

ذلك بالإضافة إلى ما تنامى حديثا من شبكات التواصل الاجتماعي والتي أصبحت عبارة عن مغناطيس للمعلومات وخاصة البيانات الشخصية والتي من خلالها يتنازل الفرد طواعية عن بياناته الشخصية للتسجيل في الموقع والحصول على حساب خاص به، ووفقا لسياسات الخصوصية والتي لا يقرأها عاده المستخدم قد يكون هناك تنازل صريح للفرد عن بياناته بالإضافة إلى ذلك أن الشخص يقوم بالإفصاح اليومي عن حالته المزاجية، صورة الشخصية، آرائه السياسية وغيرها مما يعد معلومات لا يجوز للغير الاطلاع عليها إلا بموافقة صاحب هذه البيانات ونتيجة لعدم الدراية القانونية للمستخدمين وعدم قراءه سياسات الخصوصية ينجم عن ذلك استغلال البيانات الشخصية للمستخدمين.[2]

(1) حسام شوقي، حماية وأمن المعلومات على الإنترنت، دار الكتب العلمية 2004 ص 189.

(2) Lori Andrews،Social Networks and the Death of Privacy،free press،2011، P 121 - 137

الفرع الثاني

الإنترنت أتاح عولمة المعلومات والاتصالات

في بيئة الإنترنت، تتدفق المعلومات والاتصالات عبر الحدود دون أي اعتبار للجغرافيا والسيادة، والأفراد يعطون معلوماتهم لجهات داخلية وخارجية وربما جهات ليس لها مكان معروف، وهو ما يثير مخاطر إساءة استخدام هذه البيانات خاصة في دول لا تتوفر فيها مستويات الحماية القانونية للبيانات الشخصية. وقد لا تخدم القوانين الوطنية كثيرا في هذا الفرض، كما أن تضمينها نصوصا بشأن السيطرة على نقل البيانات قد لا يكون فاعلا في ظل غياب التنسيق وضمان أن يكون نقل البيانات محكوما باتفاقات تكفل حمايتها أو تضمن توفر حماية مماثلة في الدولة المنقول لها البيانات، وتعدو المخاطر أوسع مع نشوء ملاجئ آمنة لا تقيد عمليات المعالجة بأي قيد ولا تتوفر عندها قيود منعية على جمع ومعالجة البيانات، وهي ملاجئ تهرب إليها مؤسسات الأعمال في بيئة الإنترنت للإفلات من القيود القانونية، تماما كما في حالات البحث عن ملاجئ لا تفرض فيها الضرائب أو تتيح تبادل الأموال دون رقابة، وهذه تمثل تحديا عالميا وليس مجرد تحد وطني، ولعلها الأساس الذي يدفع نحو إبرام اتفاقيات ثنائية وعالمية في حقل حماية البيانات الشخصية عبر الحدود وهو الأساس نفسه الذي أوجب إيجاد الأدوات العقدية التي تفرض على الجهة متلقية البيانات أو الوسيطة في تلقيها لإرسالها لطرف ثالث التزامات قانونية معينة تدور في مجموعها حول هدف حماية الخصوصية ومنع إساءة استخدام بيانات الأفراد الخاصة إلى جانب غرضها في منع الأنشطة الاحتيالية والمساس بالمستهلك في بيئة الإنترنت.[1]

---

(1) Anne Bliss، Ph.D.، TECHNOLOGY AND PRIVACY IN THE NEW MILLENNIUM، Ethica Publishing،2004 P163 - 199 See also Donegan، Pracilla. "Mining for knowledge." Grocery Headquarters، February 2000: p. 27 - 31.

الفرع الثالث

التحدي الناشئ عن فقدان المركزية وآليات السيطرة والتحكم

إن إقرار قانون وطني أو تطوير استراتيجية وطنية ملائمة لحماية أحد حقوق الإنسان، قد يكون فاعلا ويرجع ذلك لعنصر السيطرة والسيادة وتوفر الجهة القادرة على الرقابة ومنع الاعتداء أو استمراره، والتي تتيح أيضا التعويض وملاحقة المخالفين، لكن كيف يكون الوضع في ظل الإنترنت التي يملكها كل شخص وغير مملوكة لأحد، والتي لا تتوفر فيها سلطة مركزية ولا جهة سيادة توفر الحماية أو تتيح الفرصة والمكنة للحماية القانونية عند حدوث الاعتداء.

وبالرغم من حقيقة أن الصراع يحتدم على السيطرة على الإنترنت، من خلال السعي للسيطرة على أسماء النطاقات وعناوين المواقع، والتنافس للسيطرة على سوق استضافة المواقع عبر الخوادم التقنية والتوجه أحيانا للتحكم بالمعلومات وطرق تبادلها عبر التحكم بالحلول التقنية واحتكارها لتكون وسيلة التحكم بمصائر المستخدمين وأداة للسيطرة الفعلية، بالرغم من كل ذلك، ومع ما يرافقه من نشاط مضاد لجهة منع الاحتكار المعلوماتي وتباين المصالح بين أمريكا وأوروبا وشرق آسيا في هذا الشأن، فإن الإنترنت يتصف باللامركزية وغياب السلطة التحكمية، وليس دعوات إنشاء حكومة الإنترنت أو بوليس الإنترنت أو معايير الاستخدام الموحد أو سياسات التنظيم الذاتي للالتزامات إلا وسائل افتراضية شأنها شأن البيئة التي نشأت فيها، ومن هنا يكون لبعض مسائل التعاون الدولي أهمية بالغة، أبرزها الاتفاق في حقل الاختصاص القضائي والقانون الواجب التطبيق في بيئة منازعات الإنترنت.

ومع وجود توجهات للتعاون والتنظيم الدولي، وجهود مميزة لدى

منظمـة التعـاون الاقتصـادي والتنميـة، والاتحـاد الأوروبي، وجهـات تقنيـة وهيئـات وقطاعـات عاملـة في بيئـة الإنترنـت، فـإن كافـة هـذه الجهـود حتـى الآن لم تقـدم حلـولا لجهـة حـل مشـكلات عـدم وجـود تنظيـم مقبـول يحكـم الإنترنـت في كل مسـائله، ولعـل طبيعـة الإنترنـت واتجاهـات تطـور طريـق المعلومـات السريـع يعطـي انطباعـا أن الإنترنـت سـيبقى خـارج أمنيـات الحكومـات في إيجـاد تنظيـم قانـوني يحكمـه أو يسـيطر عـلى شـؤونه. [1]

إن البيانـات تنتقـل عـبر الإنترنـت مـن دولـة لدولـة ومـن منظمـة لمنظمـة ومـن جهـة عمـل إلى أخـرى، مـن فرد إلى مؤسسـة، دون قيـود وبكل اللغـات وتسـافر المعلومة عـبر الشـبكات المحليـة فالمناطقيـة فالدوليـة، وتوجـه مـن نقطـة لأخـرى في الفضـاء، وفي رحلتهـا هـذه تحـط وتـزور العديـد مـن مناطـق الاختصـاص القضـائي ومناطـق السـيادة، مناطـق قـد لا تكـون بينهـا تعـاون أو حتـى روابـط، ففـي مثـل هـذه البيئـة ثمـة حاجـة لجهـد اسـتثنائي عـلى النطـاق الـدولي أهـم مـا يتعـين أن يتصـف بـه الخـروج مـن الأطـر والمفاهيـم التقليديـة للسيطرة، فلـم تعـد إرادة القـوي هـي حجـر الزاويـة، فربمـا يكـون لفـرد مـا القـدرة في مثـل هـذه بيئـة أن يتحـدى أعظـم القـوى، لهـذا فـإن مـا نسـميه ديمقراطيـة الإنترنـت، وعدالـة التعامـل مـع المعرفـة، وعـدم التمييـز وانتهـاء عهد الاحتـكار والسـيطرة، هـي الأسـس التـي يتعـين أن يتـم التفكـير فيها في كل نشـاط يهدف إلى تنظيـم ضروري لمسـائل الإنترنـت، والأهـم أن يكـون تنظيـما يراعـي هـذه السـمات التقنيـة وهـذه الخصائـص وميـزات التفاعليـة اللامتناهيـة. [2]

---

(1) Jason Angiulo and Grant KleinwachterPrivacy in a Transparent WorldEthica Publishing،2010 P30 See also Chester، Jeff. Digital Destiny: New Media and the Future of Democracy. The New Press. 2007

(2) عبـد اللـه عـلى الشـنبري، التحـولات المعرفيـة الكـبرى منـذ العـصر الحجـري وحتـى جوجـل، مـدارك للنــشر،2011،ص 320.

وفي دراسة أوسع أجرتها أكبر شركات الاتصال في العالم (AT&T)[1] في نيسان 1999، أظهرت أن المستخدمين يقدمون معلومات للموقع متى ما كانت غير قادرة على التعريف بهم بشكل واف، وأن بعض المعلومات يعتبرها المستخدمين أكثر حساسية من غيرها، كأرقام بطاقات الائتمان وأرقام الضمان الاجتماعي، وأن العامل الأساسي في تقدير المستخدمين لمدى تقديم المعلومات يتوقف على إدراكهم أغراض جمعها من جهة وثقتهم أنها لن تكون محلا للتبادل مع الآخرين، وأن غالبيتهم لا يفضلون ولا يقبلون فكرة تبادل المعطيات، ولا يحبون وسائل الاتصال والتواصل غير المطلوبة ابتداء، إن توفر سياسات عامة لحماية الخصوصية في بيئة الإنترنت والتجارة الإلكترونية مترافقة مع سياسات واضحة ومعلنة من الباعة ومقدمي الخدمات يمكن أن تكون كافية لتوفير الثقة لدى المستخدمين بمستوى مقبول من حماية خصوصياتهم عبر الشبكة.

(1) AT&T Research، April 14، (1999) p.30. http://www.research.att.com/projects/privacystudy/

المطلب الثالث

مصادر تهديد خصوصية المعلومات الشخصية عبر الإنترنت

تتنوع المصادر التي تهدد خصوصية البيانات في البيئة الرقمية فمنها:

- سهولة تحديد هوية المستخدم (الفرع الأول).
- ويثار التساؤل حول مدى خطورة تقنيات اصطياد البيانات وحفظها (الفرع الثاني).
- ومدى خطورة محركات البحث وقواعد بياناتها (الفرع الثالث).

الفرع الأول

تحديد هوية المستخدم

ثمة كم هائل من الوسائل المختلفة التي يتم من خلالها تحديد هوية مستخدمي الإنترنت، بدءاً من التسجيل الأولي لمستخدمي الإنترنت من خلال مزودي خدمات الإنترنت أو في مقاهي الإنترنت، إلى ترقيم وتحديد أجهزة الإنترنت التي غالباً ما تكون مرتبطة بحسابات على الإنترنت، إلى معرفة الهوية الفردية التي توفرها متصفحات الإنترنت أو تحفظها ملفات تعريف الارتباط، فضلاً عن عناوين بروتوكول الإنترنت التي يتم تخصيصها لمستخدمي الإنترنت من خلال بروتوكولات الإنترنت، وجميع هذه الإجراءات قد تساعد على إظهار هوية مستخدم الإنترنت، ولكن في بعض الحالات قد يكون الإفصاح عن الهوية أيضاً ضروري لإتاحة الخدمات على شبكة الإنترنت، ومن الصعب استخدام الإنترنت دون وجود عنوان بروتوكول إنترنت IP على الرغم من إمكانية تخصيصه بشكل ديناميكي أو دون إظهار هويته، وتعتمد العديد من خدمات الإنترنت الأخرى كل منها على شكل من أشكال تحديد الهوية.[1]

إن من مخاوف الخصوصية في العالم النامي على وجه التحديد، وفي بعض أجزاء من العالم المتقدم، تسجيل المستخدم على الإنترنت، سواء للاستخدام قصير الأمد أو طويل الأمد، فقد يتم تعريف هوية المستخدم

---

(1) Blanchette، J.F.، & Johnson، D.G..Data retention and the panoptic society: The social benefits of forgetfulness.. The Information Society(2002؛ P 25 see alsDeighton، J.AThe Presentation of Self in the Information Age Harvard Business School Working Knowledge. (2006).P 66

كجزء من إجراءات التسجيل في مقهى الإنترنت أو كجزء من إجراءات الاشتراك في الشبكة اللاسلكية أو من خلال شراء هاتف نقال، وعلى ذلك فمثل هذا التسجيل يعرض للتنازل عن الحق في خصوصية البيانات ومن أسباب المخاوف الأخرى تقييد التعبير دون الكشف عن الهوية والتأثيرات المروعة التي تنتج عن آليات تعريف الهوية هذه.[1]

و على ذلك فإن تطوير الحواسيب الرقمية وتكنولوجيا الشبكات، وبشكل خاص الإنترنت أتاح نقل النشاط الاجتماعي والتجاري والسياسي والثقافي والاقتصادي من العالم المادي إلي العالم الافتراضي في البيئة الإلكترونية، ويوماً بعد يوم تتكامل الشبكات العالمية للمعلومات مع مختلف أنشطة الحياة، وبالوقت نفسه فإن التطور الثقافي في توظيف التقنية رافقه توجه واسع بشأن حماية خصوصية الأفراد.[2]

ففي العالم الرقمي وعالم شبكات المعلومات العالمية، يترك المستخدم آثار ودلالات كثيرة تتصل به بشكل سجلات رقمية حول الموقع الذي زاره والوقت الذي قضاه على الشبكة والأمور التي بحث عنها والمواد التي قام بتنزيلها والوسائل التي أرسلها والخدمات والبضائع التي قام بطلبها وشرائها، إنها سجلات تتضمن تفاصيل دقيقه عن شخصية وحياة وهوايات وميول المستخدم على الشبكة وهي سجلات مؤتمتة ذات محتوى شخصي يتصل بالفرد.

---

(1) رشاد عبد الله، الإنترنت في مصر والعالم العربي، ط 1،آفاق للنشر والتوزيع، 2005 ص 16.

(2) Yer - Schönberger، V. Useful Void: The Art of Forgetting in the Age of Ubiquitous Computing Faculty Research Working Papers Series: John F. Kennedy School of Government – Harvard University. (2007).Retrieved October 15، 2013 from http://ksgnotes1.harvard.edu/Research/wpaper.nsf/rwp/RWP07 - 022

والتصفح والتجول عبر الإنترنت يترك لدى الموقع المزار كمية واسعة من المعلومات على الرغم من أن جزءا من هذه المعلومات لازم لإتاحة الربط بالإنترنت والتصفح، وبمجرد الدخول إلى صفحة الموقع فإن معلومات معينه تتوفر عن الزبون وهي ما يعرف بمعلومات رأس الصفحة (header information) وهي التي يزودها الكمبيوتر المستخدم للكمبيوتر الخادم الذي يستضيف مواقع الإنترنت، وهذه المعلومات قد تتضمن[1]:

1 - عنوان بروتوكول الإنترنت العائد للزبون (IP) ومن خلاله يمكن تحديد اسم النطاق وتبعا له تحديد اسم الشركة أو الجهة التي قامت بتسجيل النطاق عن طريق نظام أسماء المنظمات وتحديد موقعها.

2 - المعلومات الأساسية عن المتصفح، ونظام التشغيل وتجهيزات النظام المادية المستخدمة من قبل الزبون.

3 - وقت وتاريخ زيارة الموقع.

4 - مواقع الإنترنت وعنوان الصفحات السابقة التي زارها المستخدم قبل دخوله الصفحة في كل الزيارة.

5 - وقد تتضمن أيضاً معلومات محرك البحث الذي استخدمه المستخدم للوصول إلي الصفحة. وتبعاً لنوع المتصفح قد يظهر عنوان البريد الإلكتروني للمستخدم.

6 - وأيضا تبعاً لتشغيل المستخدم أوامر خاصة حول إدارة التعامل مع الشبكة قد تظهر معلومات حول الوقت الذي تم قضاؤه في كل صفحة وبيان المعلومات التي أرسلت واستقبلت.

---

(1) Roger Clarke،The Supervisor›s Dilemma:Is Reconciliation Possible between،the Candidate›s Needs and the Supervisor›s Integrity?، Slovenia، (June 2013) p.231

وبالرغم من المنافع الكبيرة التي أفرزتها تكنولوجيا المعلومات وشبكات المعلومات العالمية فإنها أيضا أوجدت خطراً حقيقياً تمثل بإمكانية جمع المعلومات وتخزينها والاتصال بها والوصول إليها، وجعلها متاحة على الخط قابلة للاستخدام من قبل مختلف قطاعات الأعمال والأجهزة الخلوية بدون علم أو معرفة صاحب المعلومات.

الفرع الثاني

اصطياد البيانات الشخصية وتقنيات الكوكيز cookies

عند التطرق إلى موضوع ملفات الكوكيز المتواجدة بمتصفحات الويب، فإننا نتحدث عن عنصر مهم جدا في عالم الإنترنت ويمس بشكل كبير خصوصية جميع متصفحي الويب وبالتالي يجب بداية تعريف الكوكيز

الكوكيز: كلمة إنجليزية تعني ملفات تعريف الارتباط، وهي معلومات يتم تخزينها من قبل متصفح الويب الخاص بك عن الإجراءات التي أنجزت سابقا على موقع ما على الإنترنت. وهذه المعلومات تمكنك أن تكون أي إجراء لمشترياتك ومقتنياتك على الإنترنت، معلومات تسجيل الدخول الخاصة بك، والصفحات التي قمت بزيارتها، الأزرار التي نقرت عليها، والقائمة تطول وتطول.[1]

بالنسبة لأغلبية المستخدمين، يعتبر الكوكيز وسيلة رائعة لتوفير الوقت والطاقة والتكرار عن طريق تخزين معلومات مثل كلمات السر أو صفحات الويب التي قمت بزيارتها سابقا للحد من التكرار والكثير من إعادة كتابة المعلومات مرارا وتكرارا.

في حين أن مستخدمين آخرين يجدونها مضرة ولا يرجحون تخزين أي معلومات حول نشاطك بالويب. لحسن الحظ، هناك خطوات يمكنك اتخاذها لتعزيز خصوصيتك وإزالة ملفات تعريف الارتباط إذا كنت ترغب في ذلك، ولكن هذا يكون سلوك شخصي يستعمله المستخدم صاحب الدراية بتقنيات الإنترنت ولا تتاح للمستخدم العادي.

---

(1) Peng، Weihong; Cisna، Jennifer HTTP cookies – "A promising technology"، (2000) p.74

ويوجـد نوعـان مـن ملفـات الكوكيـز، الأول[1] Session cookies والثانيـة Persistent cookies[2].

Session cookies: وهـي نـوع مـن ملفـات الارتبـاط المؤقتـة والتي يتم مسـحها عنـد إغـلاق المتصفـح، وعنـد إعـادة تشـغيل الحاسـوب أيضـا، عنـد العـودة إلى الموقـع الـذي أنشـأ لـه ملـف الارتبـاط لـن يتعـرف عليك وسـيكون قد بـدأ دورة جديـدة عندها سـيتم إنشـاء ملفـات ارتبـط جديـدة وسـتبقى مفعلـة إلى حـين إغـلاق المتصفـح لتحـذف مـرة أخرى.[3]

Persistent cookies: هـذا النـوع مـن ملفـات الكوكيـز يتـم الإبقـاء عليـه في المجلـدات الفرعيـة بالمتصفـح حتـى تقـوم بحذفهـا يدويـا أو يحذفهـا متصفحـك اسـتنادا إلى فـترة المـدة الـواردة في ملـف تعريـف الارتبـاط.

ويتكـون ملـف الكوكيـز مـن سـتة مكونـات أساسـية هـي: تاريـخ انتهـاء مفعـول الملـف، مدتـه، الموقـع المالـك للملـف، مسـار الملـف، مـدى تشـفير الملـف.

في الحقيقـة ملفـات الكوكيـز ليسـت خطـيرة لأنهـا مجـرد ملفـات عاديـة مـن صيغـة النـص TXT، يعنـي هـذه الملفـات ليسـت بفـيروس أو شيء مـن هـذا القبيـل.

---

(1) Session Cookiea cookie that is erased when the user closes the Web browser. The session cookie is stored in temporary memory and is not retained after the browser is closed. Session cookies do not collect information from the usercomputer. They typically will store information in the form of a session identification that does not personally identify the use.

(2) Persistent Cookie: Also called a permanent cookie، or a stored cookie، a cookie that is stored on a user hard drive until it expires (persistent cookies are set with expiration dates) or until the user deletes the cookie. Persistent cookies are used to collect identifying information about the user، such as Web surfing behavior or user preferences for a specific Web site.

(3) Penenberg، Adam; Cookie Monsters، Slate، (November 7، 2005) P.43

تكمن خطورة ملفات الكوكيز في محتوياته، ليكن في علمك أن محتوياته تجمع جميع معلوماتك رقم الأي بي IP، نوع المودیم، نوع الحاسوب والمعالج، الوقت الذي تقضيه متصلا بالإنترنت، معلومات البطاقة المصرفية، والكثير الكثير. قد تعتبر هذه المعلومات التي لا تشكل خطرا كبيرا لكن ماذا لو قلت لك إن ملفات الكوكيز تحتوي على اهتماماتك أيضا.[1]

قد يستطيع أي شخص الوصول إلى بيانات المتصفح عن طريق إحدى تقنيات الاختراق مثلا استخدام تقنية sniffing للوصول إلى ملفات الكوكيز وسرقة محتواها في الوقت الذي يتم فيه تمرير ملف الكوكيز بين المتصفح والخادم ذلك بالإضافة إلى أنه يوجد المزيد من التقنيات التي تمكن المخترق للوصول إلى محتوى الكوكيز ذكرت مثالا منها.

أيضا لا ننسى الحكومات فهي أيضا تستطيع استغلال ملفات الكوكيز هذه لمعرفة جميع تحركاتك ونشاطاتك على الإنترنت فقط عن طريق طلب المعلومات من أصحاب الخادم مباشرةً.

إن تقنيات مثل (الكوكيز) يجري تخزينها بمجرد زيارة الموقع على القرص الصلب لجهاز المستخدم، وتمكن الموقع من جمع المعلومات باستمرار عن المستخدم والتي تتعلق باشتراكه على الخط والمواقع المزارة وما يفضله ومقدار مكوثه في المواقع وغير ذلك.

ففي بيئة الإنترنت، تستخدم العديد من الوسائل التقنية لتتبع المعلومات الشخصية للمشتركين [2]، من أشهرها ما يعرف برسائل (كوكيز - cookie) التي تنتقل إلى نظام المستخدم بمجرد دخوله للموقع وتتمكن من تسجيل

(1) Rouse، Margaret،"Transient cookie session cookie"،(September 2005) P.63

(2) The Center for Democracy and Technology›s Snoop Demonstration at http://snoop.cdt.org/ for an example of the information that can be easily captured by sites on the World Wide Web.

بيانات تخص المستخدم، ومع أنها كوسيلة اتبعت ابتداء لغرض غير جرمي وهو إرسال بريد إلكتروني من الشركات التجارية في إطار أنشطتها الدعائية إلى أن ذلك لا يمنع أنها تمثل كشفا عن بيانات قد لا يرغب الشخص الكشف عنها، وهي في تطوراتها اللاحقة مثلت خير وسيلة لتتبع الأشخاص وكشف حياتهم بل وإهدار توقعهم في التخفي واستخدمت لتمثل خير وسيلة لبناء دراسات التسويق وملاحقة الزبائن إلى درجة أحدثت من حالات المضايقة ما أثار التساؤل حول مدى مشروعيتها ومدى مساسها بحرية الأفراد. فشركة مثل دبل كليك Doubleclick استخدمت ما تحصلت عليه من رسائل الكوكيز لتحديد أهداف وجهة خطط الإعلان على الخط، وشركة أدفينتي Adfinity قارنت ما جمعته من معلومات حصلت عليها من مصادر أخرى على الخط فكونت بيانات متكاملة عن تصرفات المستخدمين على الخط.[1]

إن رسائل الكوكيز، وبعيدا عن فوائدها، مثلت وسيلة مهمة لملاحقة واقتفاء أثر المستخدمين وجمع المعلومات عنهم، وتحليلها لغايات الإعلان ولغايات الدراسات التسويقية على الخط. ولم تكن هذه المعلومات بعيدة عن الاستغلال في أغراض غير مشروعة أو على الأقل لا علم لصاحبها بها ولم تتح له خيارات هذا الاستخدام أو رفضه.

أما الوسيلة الأخطر فهي ما تعرف ب (برمجيات التتبع والالتقاط/ الشم) وهي وسيلة تتبع لجمع أكبر قدر من المعلومات السرية والخاصة عن طريق ما يعرف بأنظمة جمع المعلومات (تشممها).

لقد ارتكبت العديد من جهات الرقابة أنشطة إساءة استخدام البيانات الخاصة حتى في أكثر الدول المتقدمة، وكان الهدف من وراء هذه الاعتداءات في الغالب سياسيا أو اقتصاديا، لهذا كانت البيانات المستهدفة هي بيانات المعارضة السياسية والصحفيين وناشطي حقوق الإنسان، وهو ما اقتضى

---

(1) Joan E. Rigdon، "Internet Users Say They›d Rather Not Share Their «Cookies"،›WALL ST. J.، (Feb. 14، 1996) P.25

تزايـد النشـاط الـدولي في حقـل حمايـة الخصوصيـة مـن أنشـطة الرقابـة الإلكترونيـة ELETRONIC SURVEILLAN.

بـل وصـل حـد التجسـس عـلى الخصوصيـات إلى إنشـاء الـدول المتقدمـة ذاتهـا أكـبر شـبكات تجسـس مثلـت مـن الخطـورة مـا دفـع ناشـطو حمايـة الخصوصيـة في بيئة الإنترنـت إلى تنظيـم حمـلات مهاجمـة إلكترونيـة لهـذه الشـبكات بهـدف تعطيـل عملها، فقـد كشـف النقـاب عـن تطويـر وكالـة التحقيقـات الفيدراليـة برنامجـا في عـام 2000 يدعـى الملتهـم (كارنيفـور) لديـه القـدرة على التجسـس على كافـة الاتصـالات والتبادلات عـبر الإنترنـت، وأيضـا بمـا ظهـر مـن وجـود شـبكة تجسـس عالميـة أكـثر خطـورة تسـمى إيكيلـون Echelon أسسـتها وكالـة الأمـن القومـي الأمريـكي بالتعـاون مـع مؤسسـات اسـتخبارتية أوروبيـة، بهـدف التجسـس عـلى الاتصـالات الرقميـة السـلكية واللاسـلكية والاتصـالات عـبر الأقـمار الصناعيـة، وإيكيلـون نظـام عالمـي لرصـد البيانـات عبر شـبكات المعلومـات والاتصـالات، وقـد وجـه بحملـة مكثفـة مـن الاعتراضـات بلغـت حـد إعـلان يـوم محـدد لتوجيـه هجـمات بالبريـد الإلكـتروني لتعطيـل هـذه الشـبكة.

تنشـأ تهديـدات أخـرى أمـام خصوصيـة المسـتخدمين عـلى شـبكة الإنترنـت نتيجة لبرامـج الدعايـة[1] "adware" والبرمجيـات المؤذية malware والفيروسـات[2]، حيث تقوم هـذه البرامـج في بعـض الحـالات بجمع المعلومات الشـخصية للمسـتخدم واسـتخدامها في أغـراض إجراميـة، مثـل سرقـة المـال مـن الأفراد واخـتراق حسـابات الإنترنـت الخاصة بهم أو إسـاءة اسـتخدام معلوماتهـم الشـخصية بـأي طريقـة أخـرى، وتسـتخدم كذلـك برامج التجسـس بشـكل شـائع مـن قبـل المسـتخدم الراغـب في مراقبـة المسـتخدمين الآخريـن الذيـن يعرفهـم معرفة شـخصية.

---

(1) (أدوير، أو برنامج مدعوم إعلامياً) هي كل رزمة برنامج والتي تشغل، تظهر، أو تنزل إعلانات بشكل أوتوماتيكي لنظام الحاسوب بعد تنصيبها أو عند استعمالها. بعض برامج الأدوير يطلق ليها اسم سبايوير (spyware) والتي يتم تصنيفها على أنها برامج خارقة أمنياً.

(2) Braue، David (4 September 2008). "Feature: Ad - supported software". ZDNet. Retrieved 4 December 2012 P.43

وكثيراً ما تستخدم برامج التجسس هذه من جانب الملاحقين الذين يرغبون في التعدي على الحياة الشخصية لضحاياهم، وقد تتضمن نقل تفاصيل المكان الفعلي للفرد واتصالاته ومعلومات شخصية أخرى وكلمات المرور، والأمر المدهش ربما هو أنه من القانوني تماماً شراء وبيع هذه التقنيات في أجزاء كثيرة من العالم.

ولذلك، فإن من السهل نسبياً للأفراد الذين يرغبون في إساءة استخدام هذه التقنيات الوصول إليها. وتندرج برامج الدعاية ضمن فئة البرمجيات المعتدية على الخصوصية والمتجاهلة لموافقة المستخدم، وهي برمجيات يتم تخزينها على أجهزة الكمبيوتر دون قصد، وهي عبارة عن برمجيات يصعب على المستخدمين إدراكها لأنها عادة ما تظهر في شكل برنامج مكافحة الفيروسات أو أداة بحث أو تقنية مماثلة يرغب المستخدم في استخدامها، كما أنها وغالباً ما تتجمع مع البرامج التي تبدو مجانية.[1]

---

(1) دراسة استقصائية عالمية حول خصوصية الإنترنت وحرية التعبير، سلسلة اليونسكو بشأن حرية الإنترنت28/11 /2013 ص62.

الفرع الثالث

محركات البحث والاتجار بقواعد بياناتها

إن محركات البحث، تمثل الوسيلة الأهم من بين وسائل الوصول المباشر للمعلومات المطلوبة من قبل المستخدم، وهي تتباين في أدوارها ووظائفها وفعاليتها لكن ما يجمعها أنها أمست طريق المستخدمين لطلب المعلومات، فهي تتيح الوصول للموضوع ذاته أو للمواقع المهتمة بالموضوع مدار البحث، وتتيح الآن الوصول للأشخاص أو الوصول لأجزاء المعلومات، كما يتيح تطورها التقني استخدام أكثر من لغة في عملية البحث والبحث عن مواد بأكثر من لغة.[1]

وتقوم محركات البحث والأدلة الإرشادية - في تطور أوسع على شبكة الإنترنت - بعمليات جمع وتبويب وتحليل بيانات الاستخدام على نحو واسع، مستخدمة إما وسيلة الكوكيز أو غيرها من حزم النبضات / البتات اللاصقة sticky bits التي تخزن في كمبيوترات الزائرين من أجل مساعدة الموقع على التعرف على الاتجاهات الخصوصية للزائر ومساعدته في تحديد اتجاهات الإعلان وتقديم المحتويات. والمشكلة المثارة أن غالبية هذه المواقع لا تطلع المستخدم بذلك، وإن كان ثمة توجه في إطار التنظيم الذاتي لقطاعات التجارة الإلكترونية والإعلان على الإنترنت أن يتم إعلام المستخدم قبل القيام بذلك وإتاحة الخيار له للقبول والرفض.[2].

---

(1) خصوصية البيانات الرقمية، ميم: سلسلة أوراق الحق في المعرفة،مركز دعم لتقنية المعلومات 2013،نسخة إلكترونية مأخوذة من 16 2014/6/http://sitcegypt.org/?p1568

(2) Levi، Bozidar. UNIX Administration: A Comprehensive Sourcebook for Effective Systems and Network Management. CRC Press.2002 P. 207.

ومـن الممارسـات الفاضحـة في هـذا الحقـل والتـي لقيـت معارضـة واسـعة، مـا قامـت بـه شركـة إنتـل، كـبرى شركات صناعـة المعالجـات، مـن وسـم أحـد منتجاتهـا مـن الكمبيوتـرات وتمييـزه بحيـث كلـما اسـتخدم الشـخص هـذا الكمبيوتـر الموسـوم فـإن البيانـات الخاصـة بـه تظهـر عـلى نحـو يعـرف بـه ويميـزه عـن غـيره مـن المسـتخدمين.

ومـن الحـوادث الشـهيرة أيضـا، مـا أعلـن في 1998 مـن أن أحـد أكـبر مواقـع الإنترنـت التجاريـة (Double click)، سـيزود معلومـات زبائنـه - بشـأن قراراتهـم وتسـويقهم وعـادات التسـلية الخاصـة بهـم - إلى نظـام طورتـه إحـدى شركات ولايـة ماسشيوسـيتش التـي كانـت بدورهـا تتبـع أكـثر مـن 30 مليـون مسـتخدم وتسـجل مـا يقومـون بـه، ومـا يقـرؤون بـدون علـم المسـتخدمين[1].

وفي عـام 2009، ومـن بـاب التمثيـل فقـط لممارسـات البيـع التـي تسـتهدف الخصوصيـة، تـم بيـع كمبيوتـرات لا تزيـد أسـعارها عـن 1000 دولار تتيـح تتبـع مسـالك المسـتخدمين وكذلـك كافـة البيانـات عنهـم وعـن أسرهـم [2].

إن تدفـق المعلومـات وانسـيابها عـن طريـق أجهـزة الاتصـال الحديثـة وخاصـةً الكومبيوتـر والإنترنـت لـه أثـر إيجـابي في مجـال المعامـلات القانونيـة المدنيـة والتجاريـة.

ويقابـل الأثـر الإيجـابي لوسـائل الاتصـال الحديثـة أثـر سـلبي وعـلى مختلـف

---

(1) Saul Hansell، "Big Web Sites to Track Steps of Their Users"، N.Y. TIMES ABSTRACT، Aug. 16، 1998، at 1، available in 1998 WL 5422846. P.21

راجع في الموضوع نفسه لورنس م. أوليفيا، أمن تقنية المعلومات ترجمة محمد عبد الستار، مركز دراسات الوحدة العربية، 2011 ص138

(2) Karen Kaplan، In Giveaway of 10،000 PCs، the Price is Users› Privacy Marketing: Recipients Must Agree to Let Pasadena Firm Monitor Where They Go on Internet and What They Buy، L.A. TIMES، (Feb. 8،2009)، at A1 P.51

الأوضاع الاجتماعية والاقتصادية والثقافية سواء على المستوى الداخلي للدول أم على المستوى الدولي.

ولا يتوقف الأثر السلبي إلى هذا الحد، بل يمتد ليشمل حقوق الإنسان وحرياتهُ الأساسية، ومن أهم هذه الحقوق التي تعرضت للانتهاك الإلكتروني في مجال تكنولوجيا المعلومات هو الحق في الخصوصية أو الحق في الحياة الخاصة.

وقد كشفت دراسة حديثة أجرتها مؤسسة "نت نامز"، المتخصصة في مكافحة القرصنة المعلوماتية، أن 24% من البيانات المتداولة على شبكة الإنترنت مرتبطة بعمليات قرصنة لمواد محمية بحقوق الطبع والنسخ. وعزت الدراسة زيادة عمليات القرصنة إلى اتساع رقعة استخدام شبكة الإنترنت حول العالم، مشيرة إلى بعض المحاولات والحكومات حول العالم لمنع انتهاك حقوق الملكية الفكرية ولكنها تظل محاولات قليلة، في نظر القائمين على الدراسة، التي توقعت زيادة القرصنة مستقبلا.

أجريت الدراسة على مستخدمين في أميركا الشمالية وأوروبا وآسيا، حيث تم تحليل البيانات المتداولة على الشبكة العنكبوتية العامة، وعثر الباحثون على نحو 100 مليار غيغابايت من البيانات المقرصنة المتداولة، وهو ما يشكل 23.8% من إجمالي البيانات التي تم تداولها على الإنترنت في هذه الفترة، مع العلم أن النطاق المخصص لهذه النوعية من عمليات تبادل الملفات قد زاد بنسبة 160% في الفترة ما بين عامي 2010 و2012.[1]

يشار إلى أن الدراسة ركزت على نوعيات معينة من الملفات، وتحديدا المواد الموسيقية والأفلام السينمائية وألعاب الفيديو والكتب الإلكترونية.

---

(1) David Price New Study: The Size and Scope of Global Internet Piracy is on the Rise [VIDEO] of NetNames retrived http://creativefuture.org/new - study - the - size - and - scope - of - global - internet - piracy - is - on - the - rise - video/ 162014/6/

يعد كل ما يتداول على شبكة الإنترنت بيانات، اختلقت هذه البيانات من كونها شخصية أو بيانات متعلقة بتشغيل الشبكة

فتعد برامج الحاسوب أول وأهم مصنفات المعلوماتية أو تقنية المعلومات التي حظيت باهتمام كبير من حيث وجوب الاعتراف بها وتوفير الحماية القانونية لها، والبرمجيات هي الكيان المعنوي لنظام الكمبيوتر دونها لا يكون ثمة أي فائدة للمكونات المادية من الأجهزة والوسائط وهي بوجه عام تنقسم من الزاوية التقنية إلى برمجيات التشغيل المناط بها إتاحة عمل مكونات النظام معا وتوفير بيئة عمل البرمجيات التطبيقية، وتمثل البرمجيات التطبيقية النوع الثاني من أنواع البرمجيات وهي التي تقوم بمهام محددة كبرمجيات معالجة النصوص أو الجداول الحسابية أو الرسم أو غيرها، وقد تطور هذا التقسيم للبرمجيات باتجاه إيجاد برمجيات تطبيقية ثابتة وأنواع مخصوصة من البرمجيات تزاوج في مهامها بين التشغيل والتطبيق.[1]

ومن ناحية الدراسات والتشريعات القانونية فقد أثير فيها عدد من المفاهيم المتصلة بأنواع البرمجيات، أبرزها برمجيات المصدر وبرمجيات الآلة والخوارزميات ولغات البرمجة وبرامج الترجمة، وما هو يتعلق بتجميع البيانات الشخصية تعد قواعد البيانات Database هي مفتاح البيانات الشخصية والتي يمكن من خلالها تجميع الحصول على بيانات التعريف الشخصي للأشخاص ويعد هذا النوع من البرامج أو المواقع أخطر ما يهدد البيانات. وهى عبارة عن تجميع مميز للبيانات يتوافر فيه عنصر الابتكار أو الترتيب أو التبويب عبر مجهود شخصي بأي لغة أو رمز ويكون مخزنا بواسطة الحاسوب ويمكن استرجاعه بواسطته أيضا.

ومناط حماية قواعد البيانات - بوجه عام - هو الابتكار كما عبرت عنه

(1) Dawn e. Bowman،intellectual property rights and computer software، dawnsheree@aol1996 p 7

الاتفاقيات الدولية في هذا الحقل، فالمادة 10/2 من اتفاقية تربس[1] نصت على أنه: تتمتع بالحماية البيانات المجمعة أو المواد الأخرى سواء كانت في شكل مقروء آليا أو أي شكل آخر إذا كانت تشكل خلقا فكريا نتيجة انتفاء وترتيب محتواها، كما نصت المادة 5 من الاتفاقية العالمية للملكية الفكرية لسنة 1996 على أنه: تتمتع مجموعات البيانات أو المواد الأخرى بالحماية بصفتها هذه أيا كان شكلها إذا كانت تعتبر ابتكارات فكرية بسبب محتواها أو ترتيبها لكن لا تجرى كافة النظم القانونية والقوانين على هذا النهج، فالتوجيهات الصادرة عن الاتحاد الأوروبي في 11/3/1996 والقانون الفرنسي الصادر في عام 1998 لا يشترطان شرط الابتكار لحماية قواعد البيانات، بل يكفي ما بذل من جهد مالي أو بشري أو مادي وما أنفق من أجل إعداد قاعدة البيانات، وسندا لذلك فإن القانون الفرنسي المشار إليه يحمي قواعد البيانات لمدة خمس عشرة سنة ويحظر أي إعادة استعمال سواء لجزء أو لمادة كلية من قاعدة البيانات عن طريق توزيع نسخ أو الإيجار أو النقل على الخط ويحظر النقل الكلي أو الجزئي - الجوهري - من محتوى قاعدة البيانات بأي شكل، متى كان الحصول أو تقديم هذا المحتوى قد استلزم استثمارات جوهرية كما وكيفا، وسواء كان النقل دائما أم مؤقتا على دعامة بأي وسيلة أو تحت أي شكل.

والابتكار يستمد إما من طبيعة البيانات نفسها وإما من طريقة ترتيبها أو إخراجها أو تجميعها أو استرجاعها، ومحتوى البيانات في حد ذاته لا يعتبر عملا ابتكاريا، ومن هنا فإن الابتكار لا يتحقق إلا إذا عكست قاعدة البيانات سمات شخصية لواضعها، وقد قضت محكمة (نانت) التجارية الفرنسية في

(1) Agreement on Trade Related Aspects of Intellectual Property Rights:
هو اتفاق دولي تديره منظمة التجارة العالمية (WTO) الذي يحدد المعايير الدنيا للقوانين المتعلقة بالعديد من أشكال الملكية (IP) كما تنطبق على أعضاء منظمة التجارة العالمية. تم التفاوض في نهاية جولة الأوروغواي من الاتفاق العام بشأن التعريفات الجمركية والتجارة (الجات) في عام 1994.

عام 1998 بأن الابتكار الذي يتعلق بقاعدة بيانات على الإنترنت يقتضي توافر جهد جاد في البحث والاختيار والتحليل والذي عندما يقارن بمجرد التوثيق تظهر أهمية الجهد المبتكر للعمل [1].

أما قضاء محكمة النقض المصرية فإنه يتوسع في مفهوم الابتكار، فقد قضت محكمة النقض المصرية عام 1964 بأن فهرسة أحد كتب الأحاديث النبوية يعد عملا ابتكاريا لأنه يكفي أن يكون عمل واضعه حديثا في نوعه ويتميز بطابع شخصي خاص وأنه يعتبر من قبيل الابتكار في الترتيب أو التنسيق أو بأي مجهود آخر يتسم بالطابع الشخصي.[2]

وعليه، فإن البيانات أو المعلومات المخزنة في نظم الحواسيب (بشكل مجرد) ليست محل حماية، كما بالنسبة للقوانين والأنظمة وقرارات القضاء مثلا، لكنها متى ما أفرغت ضمن قاعدة بيانات وفق تصنيف معين وبآلية استرجاع معين ومتى ما خضعت لعملية معالجة تتيح ذلك فإنها تتحول من مجرد بيانات إلى قاعدة معطيات، وينطوي إنجازها بهذا الوصف على جهد ابتكاري وإبداعي يستوجب الحماية، وبتزايد أهمية المعلومات، ولما حققته بنوك المعلومات من أهمية قصوى في الأعمال والنشاط الإنساني بوصفها أمست ذات قيمة مالية كبيرة بما تمثله، وباعتماد المشروعات عليها، ولتحول المعلومة إلى محدد استراتيجي لرأس المال، بل إن البعض يراه مرتكزا لا محددا فقط، نشط الاتجاه التشريعي في العديد من الدول لتوفير الحماية القانونية لقواعد البيانات.

والاعتراف لقواعد البيانات بالحماية جاء وليد جهد واسع لمنظمة الوايبو ولمجلس أوروبا الذي وضع عام 1996 قواعد إرشادية وقرارا يقضي بالنص على حماية قواعد البيانات ضمن قوانين حق المؤلف.

---

(1) مينشار، الإنترنت والقانون، منشورات مون كريستان، 1999 باريس، ص 192.

(2) نقض مدني في 7 يوليو 1964 - مجموعة النقض المدني المصري سنة 1964، ص 920.

وهناك مئات من قواعد البيانات التي تتدفق عبر الإنترنت، وغالبيتها تحتوي على بيانات التعريف الشخصي (Personally Identifiable Information (PII لكثير منا مثال ذلك: أرقام البطاقات والحسابات البنكية وغيرها وهذا يعبر عن أن البيانات الشخصية أو بيانات التعريف الشخصي لكل منا لا تتمتع بالخصوصية المفروضة.

وفي محاولات من مالكي ومشغلي قواعد البيانات لمراقبة هذه القواعد ومواجه المشكلات التي تواجههم خاصة إذا كانت هذه القواعد تحتوي على بيانات التعريف الشخصي للأفراد - امتثالا لقوانين الخصوصية - فيقوم مديرو قواعد البيانات بالعمل بنظام إخفاء الهوية Anonymization[1] ويكون ذلك بإخفاء البيانات الشخصية الحساسة والدالة على الشخص مباشره، وذلك مثل الاسم والتليفون والعنوان والديانة[2].

ولكن البيانات الحساسة التي سيتم حذفها ستظل تحت تحكم مديري قواعد البيانات مما يدع هذا الشأن تقديريا ولا يفرض حماية كافية للبيانات، وبذلك لا يمكن أن تكون البيانات الشخصية قابله للإخفاء، لأنه لابد من وجود ثمة بيان يدل على الشخص.[3]

---

(1) Anonymization is about the methods to achieve anonymity، i.e. the removal of a person - related information that could be used for backtracking from، say، patient data to the actual patient. Anonymization is a more demanding task than pseudonymization، because even a combination of non - personal features can usually be exploited to at least narrow the choice from among a limited number of people. One network that anonymizes your web traffic through a peer - to - peer mix network doing pseudonymization and keeping your different communications apart from one another، in order to prevent combination of this data by attackers for the purpose of identification. Anonymised - to make anonymous.

(2) Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization By Michael Kassner in IT Security، September 14، (2009) P.122

(3) Paul Ohm،University of Colorado Law School،August 13، 2009،UCLA Law Review، Vol. 57، p. 1701، 2010،U of Colorado Law Legal Studies Research Paper No. 9 - 12

ومثال ذلك من الواقع العملي قد قررت شركه Group Insurance Com-mission (GIC) لإخفاء بيانات من قاعدة بيانات زيارات العاملين بالدولة للمستشفى وذلك عن طريق إزالة البيانات الخاصة بالاسم والعنوان ورقم التأمين الاجتماعي وغير ذلك فقد ظلت الكثير من البيانات المتعقلة بالموظفين متوفرة في قاعدة البيانات وذلك مثل الرقم البريدي، تاريخ الميلاد والنوع.[1]

وفي الوقت الذي تم الإعلان على أن هذه الشركة تقوم بحماية البيانات الشخصية للعملاء وقد قام باحث تقوم دراساته على الأساس الجغرافي باستخدام قاعدة البيانات والوصول منها إلى معلومات مهمة تخص محافظ الولاية.

وعلى ذلك فإما أن تكون البيانات مفيدة أو مخفية تماما وخلاصة ذلك أنه ستظل تدابير حماية البيانات أو تشريعات خصوصية المعلومات عرجاء غير ذات أثر فاعل إن لم تتحقق التكاملية ما بينها وبين ما يتعين توفره من تشريعات العصر الرقمي وتقنية المعلومات، فإدراك الحاجة إلى التكاملية ما بين تشريعات الخصوصية وتشريعات التجارة الإلكترونية وجرائم كمبيوتر والبنوك الإلكترونية وتشريعات ضبط وإقرار معايير الخدمات التقنية، وتشريعات حماية المستهلك / المستخدم للوسائل الرقمية أمر لازم لحسن التدبير وسلامة الحلول.

وثمة أحد خيارين لتحقيق التكامل وتحقيق أغراضه فإما أن يكون المنهج تقديم حزمة متكاملة من التشريعات تتواءم في بنائها معا وتدرك

---

(1) Ann Cavoukian، Ph.D. and Khaled El Emam، Ph.D.Dispelling the Myths Surrounding De - identification: Anonymization Remains a Strong Tool for Protecting Privacy، Information and Privacy Commissioner، Ontario، Canada 2011 P 9

علاقتهـا الداخليـة فيـما بينهـا وتغطـي كافـة المسـائل المسـتجدة في فـروع قانـون الكمبيوتـر ومـا يتصـل بـه، أو يصـار إلى تشريـع شـمولي يطـال كل مفـردات القانـون وتقنيـة المعلومـات.

وفي هـذه المناسـبة، يـري الباحـث أن الحـل الأمثـل للبيئـة العربيـة، التوجـه نحو وضـع تشريـع متكامـل ينظـم اسـتخدام تقنيات المعلومـات والإنترنـت بالإضافة إلى قواعد البيانـات، ومـبرر ذلـك، أن كافـة هـذه المفـردات غريبـة عـن نظمنـا القانونيـة مـن حيث المبـدأ العـام، وضمهـا معـا وتوضيـح كل حلقاتهـا سيسـاهم في إدراك المخاطبـين بأحكامها لهـذه المسـائل فـلا يقـوم الخلـط بـين مفرداتها بقـدر تعـدد تشريعاتها، ولا نكـون بحاجة في كل تشريـع لتحديـد المفاهيـم ذاتهـا، وسيسـهل علينـا عندهـا التوفيـق بـين المعايـير والمصالـح، وسـيكون التشريـع هـذا انعكاسـا لنظريـة قانـون الكمبيوتـر الواحـدة، وسـيوفر علينـا جهـود وكلفـة إنشـاء الهيئـات المتعـددة بـل والتـي أثبتـت القـراءة الأوليـة لبعـض المشـاريع القانونيـة العربيـة والقليـل الـذي أقـر في حقـل التجـارة الإلكترونيـة والملكيـة الفكريـة، إن التشـتت والتعـارض وعـدم الفعاليـة سـيكون مصـير هـذه التجـارب.

المبحث الثاني

أثر العقود الإلكترونية على خصوصية البيانات الشخصية

يعتبر العقد الإلكتروني أحد مصادر تهديد البيانات الشخصية عبر الإنترنت إذ أن تلك العقود تتطلب الإفصاح الطوعي عن البيانات الشخصية بما في ذلك من أرقام الحسابات وكذلك عند التعامل مع الشبكة ومواقع التواصل الاجتماعي يقوم الفرد طواعية بالتخلي عن حقه في خصوصية بياناته ومعلوماته الشخصية للوسيط الشبكي مع عدم توفر الحماية الكافية لمثل هذه البيانات ولدراسة أبعاد هذا التأثير.

- يثار التساؤل حول ماهية العقد الإلكتروني (**المطلب الأول**).
- وما إذا كان العقد الإلكتروني من العقود الشكلية (**المطلب الثاني**).
- وكذلك مفهوم العقود الإلكترونية من الناحية التقنية (**المطلب الثالث**).

المطلب الأول

ماهية العقد الإلكتروني

تُعد العقود التي يتم إبرامها بواسطة الوسائط الإلكترونية من أهم الموضوعات الواجب تناولها داخل القانون الذي ينظم المعاملات والتجارة الإلكترونية وكذلك تداول البيانات عبر الإنترنت، حيث إبرام تلك العقود ونفاذها، والتعبير عن إرادة المتعاقدين من إيجاب وقبول يجوز أن يتم باستخدام رسالة البيانات ما لم يتفق الطرفان على غير ذلك، كذلك فقد اعتبر أن العقد الذي يتم إبرامه باستخدام رسالة البيانات لا يفقد صحته أو قابليته للتنفيذ بسبب استخدام رسالة البيانات في إبرامه.

أيضاً اعترف القانون بصحة وسلامة العقود التي يتم إبرامها تلقائياً عن طريق الوسائط الإلكترونية طالما أن تلك الوسائط تحتوى على نظم معلوماتية معدة ومبرمجة مسبقاً للقيام بذلك التعاقد واعتبر أن تلك العقود نافذة ومنتجة لآثارها القانونية رغم عدم التدخل الشخصي المباشر أثناء عملية إبرام العقد من خلال تلك النظم.

كما أجاز القانون التعاقد الإلكتروني بين نظام معلوماتي إلكتروني مبرمج وبين شخص طبيعي آخر إذا كان الأخير يعلم أو من المفترض فيه أنه يعلم أن ذلك النظام سيتولى إبرام العقد أو تنفيذه بشكل إلكتروني تلقائي.[1]

وقبل عرض أنواع تلك العقود يجدر التنويه أن السبب في وضع تلك

---

(1) د.خالد ممدوح إبراهيم، إبرام العقد الإلكتروني،(دراسة مقارنة)، دار الفكر الجامعي، الإسكندرية 2006 ص 26. وراجع في الموضوع ذاته انظر د.إبراهيم الدسوقي أبو الليل، الجوانب القانونية للتعاملات الإلكترونية، مجلس النشر العلمي، الكويت، 2003، ص71، راجع أيضا محمد أمين الرومي، التعاقد الإلكتروني عبر الإنترنت، دار المطبوعات الجامعية، الإسكندرية، 2004، ص25.

القواعد هو حماية أطراف التعاقد الإلكتروني إذ أنه وبحسب طبيعة هذا التعاقد هو تعاقد بين طرفين غائبين عن مجلس العقد، وهذا الوضع يحتم الحرص على تحديد العديد من القواعد والمبادئ والمعلومات التي تضمن صحة وسلامة إبرامه وتجنب أي شك أو لبس فيما يتلقاه كل طرف من الطرف الأخر من رسائل بيانات أدت إلى إبرامه ويحقق من ناحية أخرى ما تتسم به المعاملات التي تتم وفقاً لهذه العقود الإلكترونية من سرعة وإنجاز دون تأخير أو تردد في إبرامها.[1]

لذلك فقد وضع القانون قواعد للتعاقد الإلكتروني بين المهنيين وأخرى بين المهنيين والمستهلكين وأخرى لعقود نقل البضائع، ويقصد بالمهني هنا كل شخص طبيعي أو معنوي يمارس لحسابه أو لحساب الغير نشاطاً يتعلق على الأخص بتوزيع أو بيع أو تأجير أو توريد السلع والخدمات.

فقد تطلب القانون أن يلتزم المهني عند تعاقده مع المهني الآخر بضرورة إخطاره أو إعلامه بطريقة واضحة ومضمونة بعدة معلومات محددة لضمان تمام التعاقد الإلكتروني بطريقة صحيحة ومنتجة لآثارها القانونية، وهى هوية وعنوان مقر ممارسة نشاطه التجاري وممثليه القانونيين، المراحل التقنية الواجب عليه اتباعها لإبرام العقد فيما بينهما، ضرورة إتاحة الوسائل التقنية التي تمكن من تحديد وتصحيح الأخطاء الوارد حدوثها عند كتابة البيانات قبل إبرام العقد، طريقة حفظ البيانات الخاصة بالعقد، والكيفية الفنية أو التقنية المتاحة للدخول إلى هذه الطريقة، اللغة أو اللغات المقترحة لإبرام العقد، وأخيراً بالمعلومات الخاصة بشهادة التوثيق الإلكتروني أو الهيئة التي أصدرتها للتأكد من صحة وسلامة التوقيع الإلكتروني في حالة استخدامه.[2]

---

(1) د. مدحت عبد الحليم رمضان، الحماية الجنائية للتجارة الإلكترونية، دار النهضة العربية 2001 ص 36().

(2) أمير فرج يوسف، عالمية التجارة الإلكترونية وعقودها، المكتب الجامعي الحديث، الإسكندرية،2009 ص 259.

وجدير بالذكر في هذا المقام أن المعلومات المشار إليها هي الحد الأدنى من المعلومات الواجب الإحاطة بها لدى طرفي التعاقد وبالتالي يجوز إضافة معلومات أخرى عليها.

والبين من المعلومات المذكورة أنها تتعلق كلها بمسائل شكلية أو إجرائية تضمن سلامة إبرام العقد فيما بين المهنيين وتغطى القصور الذي تواجد نتيجة عدم تواجدهما في مجلس واحد للعقد وأنهما تعاقدا بواسطة الوسائط الإلكترونية كما تضمن من جهة أخرى صحة التراضي بين طرفي العقد وهو أحد أهم أركان التعاقد بصفة عامة. تطرق القانون بعد ذلك للتعاقد الإلكتروني بين المهنيين من جهة والمستهلك من جهة أخرى، ووضع أيضاً حدا أدنى من القواعد الواجب توافرها في مثل هذه النوعية من العقود مراعياً في ذلك حماية المستهلك في مثل هذه النوعية من العقود التي لا تسمح له - بحكم طبيعتها - من إحاطته التامة بكافة جوانب الخدمة أو السلعة محل التعاقد أو بما يجب أن يقوم به من إجراءات أو أساليب احترازية لضمان عدم وقوعه في أي عيب من عيوب الرضاء. فالمستهلك في هذه العقود لا يألف التعاقد الإلكتروني كما هو الحال بالنسبة للمهنيين المتمرسين بحكم طبيعة عملهم على إبرام العقود الإلكترونية ويدركون كل تفاصيلها ومخاطرها، وبالتالي فهو في حاجة إلى مزيد من الحماية القانونية له عند الإقدام على التعاقد الإلكتروني. [1]

يتميز العقد الإلكتروني بصفته العالمية التي تغطي كل دول العالم لكونه يتم في معظم الأحيان عن طريق شبكة المعلومات (الإنترنت) كما يتميز أيضا بصفته الانفتاحية فالشبكة متاحة لكل من يرغب الدخول فيها، ويتميز العقد الإلكتروني أخيرا بصفته الإلكترونية لكونه يتم بواسطة أجهزة وبرامج

(1) نزيه محمد المهدي، الالتزام قبل التعاقد الإدلاء بالبيانات المتعلقة بالعقد وتطبيقاتها على بعض أنواع العقود، دار النهضة العربية،2000 ص 23. راجع في السياق ذاته د.أسامة أبو الحسن مجاهد، التعاقد عبر الإنترنت، دار الكتب القانونية، المحلة الكبرى، 2002، ص11.

إلكترونيـة تنقـل إرادة المتعاقديـن بعضهـم إلى بعـض دون حضـور مـادي معـاصر لهـم وبالتـالي فهـو عقـد ينتمـي إلى طائفـة العقـود عـن بعـد.[1]

وقـد عـرف التوجيـه الأوروبي الصـادر في 20 مايـو 1997 والمتعلق بحماية المسـتهلك في العقـود المبرمـة عـن بعـد Remote Contract بأنـه: " عقد متعلـق بالسـلع والخدمات يتـم بـين مـورد ومسـتهلك مـن خـلال الإطـار التنظيمـي الخـاص بالبيـع عـن بعـد أو تقديـم الخدمـات التـي ينظمهـا المـورد والذي يتـم باسـتخدام واحدة أو أكثر من وسـائل الاتصـال الإلكترونيـة remote communications حتـى إتمـام العقـد".

وعرفـه جانـب مـن الفقـه الأمريـكي بأنـه:" هـو ذلـك العقـد الـذي ينطـوي عـلى تبـادل للرسـائل بـين البائـع والمشـترى والتي تكـون قائمة على صيـغ معدة سـلفا ومعالجة إلكترونيـا وتنشـئ التزامـات تعاقديـة "[2].

ويعـرف بعـض الفقـه اللاتينـي العقـد الإلكـتروني بأنـه: " اتفـاق يتلاقـى فيـه الإيجـاب والقبـول عـلى شـبكة دوليـة مفتوحـة للاتصال عن بعد وذلك بوسـيلة مسـموعة مرئيـة، وبفضـل التفاعـل بـين الموجـب والقابـل "[3]

ويأخـذ بعـض الفقـه[4] عـلى هـذا التعريـف أنه جـاء ناقصـا، حيث لم يبـين النتيجة المترتبـة عـلى التقـاء الإيجـاب والقبـول، وهـى إحـداث أثـر قانـوني وإنشـاء التزامـات تعاقديـة.

(1) Making and Enforcing Contracts، Online، Provided by the Association of Corporate Counsel، 1025 Connecticut Avenue، NW، Suite 200، Washington، DC 20036 USA (September 2012) P.144

(2) Michael. s. Baum & Henry. h. Perritt، Electronic contracting، op.cit P.132

(3) د. أسامة أبو الحسن مجاهد، خصوصية التعاقد عبر الإنترنت، دار النهضة العربية، 2000، ص39.

(4) د. خالد ممدوح إبراهيم، إبرام العقد الإلكتروني، دار الفكر الجامعي، 2006 ص42.

وحيث إن العقد الإلكتروني عبر شبكة الإنترنت يتميز بأنه يتم في الغالب على المستوى الدولي فقد ذهب البعض إلى تعريف عقد التجارة الإلكتروني الدولي بأنه: "العقد الذي تتلاقى فيه عروض السلع والخدمات بقبول من أشخاص في دول أخرى، وذلك من خلال الوسائط التكنولوجية المتعددة ومنها شبكة الإنترنت بهدف إتمام العقد "[1]. وتجدر الإشارة إلى أن عملية التعاقد الإلكتروني تشتمل بخلاف الإيجاب والقبول على العديد من المعاملات الإلكترونية مثل العروض والإعلان عن السلع والخدمات وأوامر الدفع الإلكترونية وغير ذلك.

ومما سبق يمكن أن نعرف العقد الإلكتروني تعريفا موجزا يتفادى الانتقادات الموجهة للتعريفات السابقة وذلك بقولنا إن العقد الإلكتروني هو: "العقد الذي يتم انعقاده بوسيلة إلكترونية بقصد إنشاء التزامات تعاقدية "[2].

(1) أحمد عبد الكريم سلامة، القانون الدولي الخاص النوعي (الإلكتروني، السياحي، البيئي)، دار النهضة العربية، ط1، 2002 ص53.

(2) على صعيد التشريعات العربية لا نجد تعريفا للعقد الإلكتروني إلا في قانون المعاملات الإلكترونية الأردني رقم 85 لسنة 2001 حيث يعرفه في المادة 2 بأنه: الاتفاق الذي يتم انعقاده بوسائل إلكترونية، كليا أو جزئيا.

المطلب الثاني

الشكلية في التعاقد الإلكتروني

الأصل في العقود هو الرضائية، بمعنى أن العقد يبرم بمجرد أن يتبادل المتعاقدان التعبير عن إرادتيهما دون حاجة إلى إجراء آخر، وينطبق ذلك بطبيعة الحال على العقد الإلكتروني.[1]

واستثناءً من ذلك قد يتطلب القانون إفراغ التراضي في شكل محدد وهو ما اصطلح على تسميته بالعقود الشكلية[2].

والعقود الشكلية: هي مجموعة العقود التي لا يكفي لإبرامها مجرد التراضي وإنما يشترط فيها القانون مراعاة [3]شكل خاص بدونه لا يوجد العقد قانونا، ولا يرتب أثرا ولا يمكن الاحتجاج به.

والشكل الذي تشترطه القوانين المعاصرة غالبا ما يكون الكتابة في ورقة رسمية يقوم بتحريرها شخص مكلف قانونا، وهو الموثق الرسمي أو محرر العقود. ومثال العقود الرسمية "الشكلية" هبة العقار والكتابة باعتبارها ركنا لا يتم التعاقد إلا به تستدعي تمييزها عن الكتابة اللازمة للإثبات.[4]

ففي الحالة الأخيرة ينعقد العقد ويرتب آثاره كاملة في مواجهة أطرافه غير أنه إذا ثار نزاع بشأنه تكون الكتابة لازمة للإثبات[5].

---

(1) ا د.عباس العبودي، التعاقد عن طريق وسائل الاتصال الفوري وحجيتها في الإثبات المدني، دار الثقافة للنشر والتوزيع، عمان، 1997 م، ص35.

(2) د.السنهوري، نظرية العقد، الجزء الأول، ط1، 1934 م، القاهرة، ص79

(3) محمد أمين الرومي، التعاقد الإلكتروني عبر الإنترنت، دار المطبوعات الجامعية، الإسكندرية، 2004، ص87.

(4) . د.إسماعيل غانم، النظرية العامة للالتزامات، القاهرة، 1966 ص 32.

(5) د. محمد جمال عطية، الشكلية القانونية، دراسة مقارنة، رسالة دكتوراه، كلية الحقوق، جامعة الزقازيق، 1993، ص183.

وأحب أن أشير في هذا المقام إلى أن البعض يخلط بين الإجراءات التي يشترطها المشرع في بعض الأمور لأهميتها كتسجيل عقود بيع العقارات وفقا لأحكام التسجيل العقاري وبين الشكلية، حيث يعتبر تلك الإجراءات من قبيل الشكلية. والذي نراه - منضمين في ذلك إلى بعض الفقه[1] - أن التسجيل ليس ركنا شكليا في العقد.[2]

ولا تتوقف صحة العقد على وجوده، وإنما هو شرط لإمكان تنفيذ البائع لالتزامه، فلا تنتقل الملكية للمشتري إلا بتسجيل العقد، وهنا يظهر الفارق بين الركنية في العقد وغيرها، فلو كان التسجيل ركناً لما وجد العقد، ولكنه باعتباره ليس كذلك فإن العقد يكون صحيحا ويجوز للمشتري إلزام البائع بالقيام بإجراءات التسجيل العقاري حتى تنتقل له ملكية العقار،

فإن رفض البائع ذلك جاز للمشتري المطالبة قضاء بالحكم له بصحة ونفاذ العقد، فإذا ما حكم له بذلك سجل حكمه وحق له طلب تثبيت ملكيته استناد إلى الحكم الذي يقوم مقام العقد بعد تسجيله.

وإذا كان هذا هو مفهوم الشكلية يحق لنا التساؤل حول إمكانية استيفاء الشكلية بالطريقة نفسها عند إبرام العقد الإلكتروني ؟ بمعنى هل مناط الشكلية الكتابة على الورق أم أنها تستوعب الكتابة الإلكترونية ؟ وهل يقوم التوقيع الإلكتروني مقام التوقيع العادي الذي يشترطه القانون في بعض الأحيان ؟

وفيما يلي الإجابة عن هذه التساؤلات:

العقد الإلكتروني عندما يشترط القانون شكلا معينا بعد صدور القانون رقم 2000/230 في فرنسا بشأن تطوير قانون الإثبات والمتعلق

---

(1) أ. رامي علوان، بحث بعنوان: "التعبير عن الإرادة عن طريق الإنترنت وإثبات التعاقد الإلكتروني "، مجلة الحقوق، ع 4، س26، ديسمبر 2002 ص23.

(2) د. بشار طلال مومنى، مشكلات التعاقد عبر الإنترنت، رسالة دكتوراه، كلية الحقوق، جامعة المنصورة، 2003.

بالتوقيع الإلكتروني انقسم الرأي بين مؤيد ومعارض، فقد ذهب البعض إلى أن الشكلية التي يتطلبها القانون لانعقاد العقد أو التصرف سواء بالكتابة أو بالتوقيع لا يمكن أن يستغنى عنها بالكتابة الإلكترونية أو التوقيع الإلكتروني وأن التعديل لنص المادة (1/1316)[1] مدني فرنسي يتحدث عن الكتابة كوسيلة إثبات ولم يقصد المساس بالشكلية.

وبالتالي من غير المتصور أن تعقد تصرفات إنشاء الوصية أو الوقف أو معاملات التصرف في الأموال ومعاملات الأحوال الشخصية على الخط، وذلك بسبب أهمية هذه التصرفات وخطورتها[2].

بينما يذهب البعض الآخر إلى أن الكتابة الإلكترونية لم تعد مقصورة على الكتابة كوسيلة إثبات، وإنما تشمل الكتابة كشرط لصحة التصرف وذلك بالنظر إلى عمومية نص المادة (1/1316) مدني فرنسي، فالنص واضح فيما تضمنه من تعريف للكتابة ولذلك يجب إعطاءه معنى كاملا دون تخصيص[3].

ومن الجدير بالذكر أن التوجيه الأوروبي رقم 2000/31 بشأن التجارة الإلكترونية حظر على الدول الأعضاء وضع أي عراقيل أو عقبات أمام الاعتراف بالعقود الإلكترونية وحثهم على العمل على تطوير تشريعاتها لإقرار المعاملات الإلكترونية، ولا شك أن عدم منح الكتابة الإلكترونية قوة ترتيب كافة الآثار القانونية يكون مخالفا لمقتضيات الجماعة الأوروبية.[4]

ويرى الباحث انضماما إلى أصحاب الرأي الأول فيما يذهبون إليه، فلا

---

(1) تنص المادة (1/1316) من القانون المدني الفرنسي على أنه: " ينشأ الإثبات الخطي أو بالكتابة من تتابع أحرف أو أشكال أو أرقام أو أية إشارات لها دلالة قابلة للإدراك، وذلك أيا كانت دعامتها أو الوسائل المستخدمة في نقلها".

(2) أ. رامي علوان، المرجع السابق، ص268

(3) د. محمد حسن قاسم، التعاقد عن بعد، دار الجامعة الجديدة للنشر، الإسكندرية، 2005، ص105.

(4) محمد حسين منصور، المسؤولية الإلكترونية، دار الجامعة الجديدة للنشر، الإسكندرية، 2003، ص150.

يستساغ عقلا ولا منطقا أن تبرم عقود في غاية الأهمية والخطورة عن بعد، وأن يضرب باشتراطات القانون عرض الحائط. ولعل عدم كفاية الوسائل التقنية في توفير الثقة والأمان في إبرام هذه العقود وهو ما يرجح هذه الوجهة.

وتشريعيا نقرأ في قانون التوقيع الإلكتروني المصري رقم 15 لسنة 2004 مبدأً عاماً قررته المادة (15) من هذا القانون بقولها: "للكتابة الإلكترونية وللمحررات الإلكترونية في نطاق المعاملات المدنية ذات الحجية المقررة للكتابة والمحررات الرسمية والعرفية في أحكام قانون الإثبات في المواد المدنية والتجارية متى استوفت الشروط المنصوص عليها في هذا القانون وفقاً للضوابط الفنية والتقنية التي تحددها اللائحة التنفيذية لهذا القانون".[1]

والنص واضح في كونه أقر إمكانية استيفاء الشكلية التي يقررها القانون لإبرام العقد أو لترتيب آثاره عن طريق المحررات والمستندات الإلكترونية متى روعيت الشروط التي حددها المشرع في اللائحة التنفيذية للقانون. وقد أقر هذا المبدأ أيضا في كل من القانون الأردني للمعاملات الإلكترونية (م7) وقانون إمارة دبي للمعاملات والتجارة الإلكترونية (م9).[2]

إذن نخلص من خلال هذا العرض أن أغلب التشريعات تتبنى مبدأ المساواة بين الكتابة الإلكترونية والكتابة التقليدية، والتوقيع الإلكتروني والتوقيع التقليدي، ولكن الإشكالية تثور عندما يستلزم القانون شكلا معينا لانعقاد التصرف.

وبالتالي فإن العقود الإلكترونية التي يبرمها المستخدم عن طريق التخلي عن بياناته الشخصية وكذلك ملئ نماذج معدة سلفا يعد رضاء واضحا منه

---

(1) د. محمد جمال عطية، الشكلية القانونية، دراسة مقارنة، رسالة دكتوراه، كلية الحقوق، جامعة الزقازيق، 1993، ص183.

(2) د. عبد الله بن إبراهيم الناصر:" العقود الإلكترونية، دراسة فقهية تطبيقية مقارنة "، بحث مقدم إلى مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون والمقام بدولة الإمارات العربية المتحدة في الفترة من 10 _12 مايو 2003.

على إبرام هذا العقد الإلكتروني، ويسمح للطرف الأخر في هذا العقد بل ويعطيه الحق في الاطلاع وتخزين ومعالجه البيانات الذي تخلى عنها في مقابل إبرام العقد، حتى وإن كانت تلك البيانات لا تعد ركنا جوهريا في إبرام العقد ولكن الشكلية في عقود الإنترنت جعلت منها ركنا أساسيا وقد يقوم مقدم الخدمة فيما بعد باستغلال هذه البيانات وبدون علم المستخدم وهو ما يهدد خصوصية البيانات الخاصة به، وقد تكون الاستمارات يملؤها المستخدم معدة سلفا لجمع البيانات لاستغلالها في أغراض تسويقية أو غيرها.

المطلب الثالث

العقود الإلكترونية من الناحية التقنية

العقـود الإلكترونيـة Web Wrap Agreement أو Click wrap Contracts

قبـل أن يكـون هنـاك صفحـات إنترنـت web pages، كان هنـاك البرمجيـات، وتمامـا كـما أصبح لصفحـات الويـب، عقـود ويـب (web wrap agreements) فقد كان للبرمجيـات الجاهـزة (software) عقودا مشـابهة سـميت (shrink wrap agreement) وعقـود (shrink wrap agreement)، هـي اتفاقيـات الرخـص (النقـل) الرخـص التـي ترافـق البرامـج، وهـي على شـكلين:

الأول: التـي لهـا رخـص تظهـر عـلى الشاشـة أثنـاء عمليـة تنزيـل البرنامـج عـلى الجهـاز، وعـادة لا يقرؤهـا المسـتخدم، بـل يكتفـي بمجـرد الضغـط (أنـا اقبـل I agree) أو (I accept)، إنهـا العقـد الإلكـتروني الـذي يجد وجوده في واجهـة أي برنامـج ويسـبق عمليـة التنزيـل (Install).[1]

أمـا الصـورة الثانيـة: وهـي السـبب في أخذهـا هـذا الاسـم (الـذي يعنـي رخصة فض العبـوة) فإنهـا الرخـص التـي تكـون مـع حزمـة البرنامـج المعروضـة للبيـع في محـلات بيـع البرمجيـات، وعـادة تظهـر هـذه الرخصـة تحـت الغـلاف البلاسـتيكي عـلى الحزمـة وعـادة تبـدأ بعبـارة (بمجـرد فـض هـذه العبـوة، فانـك توافـق عـلى الـشروط الـواردة في الرخصـة) ومـن هنـا شـاع تعبـير (رخصـة فـض العبـوة).[2]

---

(1) Epstein، Michael A. (2006). Epstein on Intellectual Property. Aspen Publishers Online. pp. 11-19.

(2) Nancy Kim، CLICKING AND CRINGING: MAKING SENSE OF

وكانت هذه الطريقة في حقيقتها طريقة مقنعة للتعاقد، لكنها لم تكن يوما طريقة واضحة، ولم تكن تشعر أن العقد ملزم، لأن أحدا لم يكن يهتم بقراءة الرخصة قبل فض العبوة، ولا حتى بعد فضها، وربما عدد محدود من الأشخاص ممن احتفظوا بالرخصة نفسها، ومن هنا رفضتها المحاكم في المرحلة الأولى. لكن وفي الفترة الأخيرة، وتحديدا في عام 1998 وفي إحدى القضايا وهي الأشهر من بين قضايا رخص فض العبوة، وهي قضية Pro CD v. Zeidenberg[1]، قضت محكمة الاستئناف الأمريكية / الدائرة السابعة، بقبول حجية هذا العقد قياسا على العقود التي لا يجري معرفة شروط التعاقد إلا بعد الدفع فعلا كتذاكر الطائرة، وبوالص التامين.

هذا العقد - عقد فض العبوة - مثل الأساس التاريخي والعملي لعقود الويب أو العقود الإلكترونية، وسيكون لهذا العقد دور آخر في حقل العقد الإلكتروني عندما يكون محل القياس لدى بحث قانونية العقود الإلكترونية وسيجري قياس العقد الإلكتروني في قيمته القانونية أمام المحاكم الأمريكية.[2]

ويعد العقد Wrap Click Contract الصورة الأكثر شيوعا

CLICKWRAP، BROWSEWRAP AND SHRINKWRAP LICENSES، online article،available https://www.law.stanford.edu/sites/default/files /event/266730/media/slspublic/Kim_clicking_and_cringing.pdf،See alsoRobert A. Hillman، Online Boilerplate: Would Mandatory Website Disclosure of E - Standard Terms BackfireوMICH. L. REV. 2003، p 9

(1) ProCD، Inc. v. Zeidenberg، 86 F.3d 1447 (7th Cir. 1996)، is a United States contract case involving a "shrink wrap license". One issue presented to the court was whether a shrink wrap license was valid and enforceable. Judge Easterbrook wrote the opinion for the court and found such a license was valid and enforceable. The Seventh Circuit›s decision overturned a lower court decision.

(2) Article Jones Day،The legacy of ProCD v. Zeidenberg، Software License Jurisprudence، 2004 P 2

للعقد الإلكتروني وهو عقد مصمم لبيئة النشاط (على الخط) كما في حالة الإنترنت، وذلك بوجود (وثيقة) العقد مطبوعة على الموقع متضمنة الحقوق والالتزامات لطرفيه (المستخدم وجهة الموقع) منتهية بمكان متروك لطباعة عبارة القبول أو للضغط على إحدى العبارتين (أقبل) أو (لا أقبل) أو عبارات شبيهة، وترجع تسميته المشار إليها إلى حقيقة أن إبرام العقد يتم بالضغط (click) على أداة الماوس، إما على أيقونة الموضع المتضمنة عبارة (أنا اقبل) أو في المساحة المخصصة لطبع هذه العبارة لغايات وضع المؤشر فيها عبر الضغط بالماوس.[1]

ويستخدم العقد الإلكتروني لكافة التصرفات محل الاتفاقات على الشبكة، وبشكل رئيس:

إنزال البرامج أو الملفات من الشبكة، الدخول إلى خدمات الموقع وتحديدا التي تتطلب اشتراكا خاصا في بعض الأحيان أو مقابل مالي أو لغايات الحصول على الخدمة (كالمحادثة ومجموعات الأخبار أو الإعلان والأدلة) أو لغايات التسجيل والالتزام العقدي بإنفاذ الخدمة المعروضة مجانا بشروط الموقع كخدمات البريد المجاني والاستضافة المجانية وغيرها. وكذلك لإبرام التصرفات القانونية على الخط كالبيع والشراء والاستئجار وطلب القرض وإجراء عملية حوالة مصرفية وإبرام بوالص التأمين ودفع الثمن وغيرها.[2]

ومن حيث أهمية العقد الإلكتروني، فإن تقنية العقود الإلكترونية توفر قدرة التعاقد على الشبكة وفي بيئتها والحصول على الخدمات والبضائع

(1) Rachel Cormier Anderson، Enforcement of Contractual Terms in Clickwrap Agreements، Shidler J. L. Com. & Tech. 11 (Feb. 14، 2007)، at http://www.lctjournal.washington.edu/Vol3/a011Cormier.html

(2) د. محمد أمين الرومي، التعاقد الإلكتروني عبر الإنترنت، الطبعة الأولى، دار المطبوعات الجامعية، الإسكندرية 2004.ص97. و راجع في السياق ذاته د. ممدوح محمد علي مبروك، مدى حجية التوقيع الإلكتروني في الإثبات، دار النهضة العربية، القاهرة. ص36. و أحمد خالد العجلوني، التعاقد عن طريق الإنترنت، رسالة ماجستير، 2002. ص 115.

والمصنفات بأرخص الأسعار ومن خلال قوائم اختيار معروفة وواسعة ومن أي موقع أو مصدر للموردين على الخط[1] (OSP)، كما تتيح للمورد تحديد التزاماته بوضوح، وتحديد نطاق المسؤولية عن الخطأ، والأضرار جراء التعاقد أو بسبب محل التعاقد كأخطاء البرمجيات ومشاكلها، وتساهم في تسهيل المقاضاة بين الطرفين لما تقرره من قواعد شاملة بالنسبة للحقوق والالتزامات.[2]

---

(1) OSP: All of the telecommunications apparatus and cable systems outside (i.e.، not housed in buildings) such as central offices or customer premises. OSP includes all the components of cable systems such as the aerial، buried، and underground cables، amplifiers and repeaters، cross - connect boxes، and remote neighborhood nodes، some of which may be located in vaults or sheds. See also inside plant. An online service provider can، for example، be an Internet service provider، email provider، news provider (press)، entertainment provider (music، movies)، search، e - shopping site (online stores)، e - finance or e - banking site، e - health site، e - government site، Wikipedia، or Usenet.[clarification needed] In its original more limited definition، it referred only to a commercial computer communication service in which paid members could dial via a computer modem the service›s private computer network and access various services and information resources such a bulletin boards، downloadable files and programs، news articles، chat rooms، and electronic mail services. The term "online service" was also used in references to these dial - up services. The traditional dial - up online service differed from the modern Internet service provider in that they provided a large degree of content that was only accessible by those who subscribed to the online service، while ISP mostly serves to provide access to the Internet and generally provides little if any exclusive content of its own.

(2) د. سمير حامد عبد العزيز الجمال، التعاقد عبر تقنيات الاتصال الحديثة، الطبعة الأولى، دار النهضة العربية، القاهرة 2000. ص 88.

وتتعـدد أنـواع العقـود الإلكترونيـة مـن حيـث آليـة إبرامهـا: ويمكـن ردهـا بوجه عـام إلى طائفتـين، إمـا عقـود تتـم بمجرد الضغـط عـلى أيقونة (مربـع/ مسـتطيل) القبول وتسـمى (Icon Clicking). أو عقـود تتـم بطباعـة العبـارة التي تفيـد القبول (Type & Click). أمـا مـن حيـث المحـل فتمتـد إلى أنـواع غـير حصريـة باعتبارهـا تتعلـق بمنتجات وخدمـات وطلبات.



وقـد بحثـت العديـد مـن المحاكـم في النظـم القانونيـة المقارنـة لحجيـة هـذه العقـود، وتباينـت الاتجاهـات بشـأنها قبـل أن يتـم تنظيـم حجيتهـا قانونـا في عـدد مـن الـدول، أو الاسـتعداد التشريعـي في عـدد آخـر تمهيـدا لقبولهـا وإقـرار حجيتهـا ضمـن شروط ومعاييـر معينـة، ويمكـن القـول إن الاتجـاه العـام قبـل التدخـل التشريعـي أجـاز قبـول هـذه التعاقـدات قياسـا عـلى تراخيـص فـض العبـوة في حقـل البرمجيـات، وذلـك ضمـن شروط أهمهـا وأولهـا أن يكـون متاحـا بيسـر الاطلاع عـلى شروطهـا وقراءتها وتوفر خيـارات الرفـض والقبـول، وأن يتعـزز القبـول بإجراء أكـثر من مجرد الضغـط على الماوس في حالـة النـوع الأول مـن هـذه العقـود المشـار إليه أعـلاه. وأضافـت بعـض المحاكم شرط اعتماديـة وسـائل التعريـف بشـخصية المسـتخدم إلى جانـب وسـائل الأمـان[1].

---

(1) (قضيـة Hotmail Corp v. Van Money Pic 1998 وقضيـة ProCD،

إن مشكلات عقود الإنترنت ابتداء من عقود الاشتراك في الخدمة مرورا بالعقود ذات المحتوى التقني، وعقود الجهات ذات العلاقة بمواقع الإنترنت أو عقود المستخدمين مع المواقع بما فيها عقود طلب الخدمات والتسوق الإلكتروني وعقود الخدمات المدفوعة والمجانية كعقود البريد الإلكتروني ورخص استخدام وتنزيل البرامج وعقود ورخص نقل التكنولوجيا وغيرها من العقود التي تقع في نطاق العقود الإلكترونية أو العقود المبرمة عبر المراسلات الإلكترونية كلها تندرج تحت العقود والتصرفات المتصلة بالإنترنت فهي تتعلق بالتنظيم القانوني للتعامل مع الإنترنت[(1)]

وكل هذه الأنواع من العقود تتطلب التنازل عن بعض البيانات الشخصية للمستخدم، وحماية تلك البيانات تكون مندرجة تحت القوانين التي تحكم العلاقة التعاقدية وتحكم بيئة الإنترنت، علما بأن العقد الإلكتروني يتطلب الإفصاح عن معلومات أكثر من المطلوبة عند إبرام العقود العادية، فمثلا فإن البيع والشراء والدخول في المزادات في الواقع الحقيقي قد لا يتطلب أكثر من تحديد الدافع، وهي بذاتها تنطوي على سمات التخفي أكثر من وسائل الدفع التي تتطلب تقديم معلومات، خاصة إن كان تقديمها يتم للغير. وفي بيئة الإنترنت، فإن وسائل الدفع السائدة تتمثل بالبطاقات المالية، فتتطلب عمليات الشراء وعمليات الإعلان وطلب الخدمات والمزادات في العالم التخيلي - الإنترنت - تقديم اسم الشخص ورقم هاتفه وعنوانه وبريده الإلكتروني، وببساطة فإنها تتطلب معلومات تفصيلية يغيب فيها القدرة على التخفي خلافا للعالم الواقعي.

ولهذا فإن حماية خصوصية التعاملات المالية في بيئة الإنترنت أحد أهم ضمانات وجود النشاط التجاري فيها وتطوره، وكما قيل فإن نظام الدفع

Inc. v. Zeidenberg 1996 وقضية Hill v. Gateway 2000 Inc. 1997 & Brower v. Gateway 2000 Inc. 1998)

(1) انظر: د. حسام الدين الأهواني - حماية حقوق الملكية الفكرية في مجال الإنترنت، ورقة عمل مقدمة إلى مؤتمر الملكية الفكرية - جامعة اليرموك - الأردن 10 - 2000/7/11.

المالي على الإنترنت بدون نظام حماية للخصوصية سينقلنا من عالم الدفع النقدي المستتر إلى عالم مليء بوسائل الكشف والتعريف تتزايد فيه قدرة تتبع الأشخاص[1].

و نخلص مما سبق إلى أن الأساس في التعاقد الإلكتروني هو تخلي المتعاقد مع الجهة الإلكترونية غير المرئية هو التنازل والإفصاح عن بياناته الشخصية ويجب أن يكون على دراية أن مثل تلك البيانات لن تتوقف عند سجلات هذه الجهة أو الموقع إذ أن احتمال إعادة استغلال مثل هذه البيانات يكاد يكون حقيقة سواء تم شراء قاعدة البيانات لأغراض تسويقية أم سياسية أم استخدامها في دراسات تحليلية سواء من قبل شركات أم جهات حكومية فإن مثل الإفصاح الطوعي يجب أن يكون مشروطاً للاستخدام في نطاق العقد، وقد يكون هذا منطقياً إلا أنه في واقع الأمر غير قابل للتحقيق في ظل تسرب المعلومات على شبكة الإنترنت، ومن ثم فمع عدم القدرة الدولية على وضع ضوابط وعدم قدرة بعض الأجهزة السيادية على وضع إطار قانوني عادل وصارم لمراقبة السلوك على الإنترنت لا يمكن تحقيق ذلك.

---

(1) FRB: Federal Reserve Board Speech from Mar. 7، 1997 http://www.bog.frb.fed.us/boarddocs/speeches/19970307.htm (remarks by Federal Reserve Board Chairman Alan Greenspan at the Conference on Privacy in the Information Age، Salt Lake City، UT، Mar. 1997). A. Michael Froomkin، Flood Control on the Information Ocean: Living with Anonymity، Digital Cash، and Distributed Databases، 15 J.L. & COM. 395، 471 (1996). Minimum Security Devices and Procedures and Bank Secrecy Act Compliance، 63 Fed. Reg. 67،529,67،536 (Dec. 7، 1998). Declan McCullagh، Banking With Big Brother، Wired News http://www.wired.com/news/print_version/politics/story/16749.html?wnpgall

المبحث الثالث

الإطار الأساسي لمبادئ خصوصية المعلومات المعترف بها

إن حماية الخصوصية في البيئة الرقمية عملية وليست مجرد إجراء، وبقدر الإحاطة بأهمية الحماية وفعالية وسائلها بقدر ما يتحقق إتاحة الثقة بالتقنية لدى مستخدميها، وتوفر الثقة هو العنصر الأول والرئيس لتسهيل الاندماج بالمجتمع الرقمي وتجلياته، وإن وضع إطار لحماية الخصوصية الذي يتيح تجاوز تهديداتها والتشجيع على الاندماج في المجتمع الرقمي.

وعندما نقول إنها عملية وليست مجرد إجراء، فإن هذا يعني أنها تنطلق من رؤيا محددة المعالم واضحة الأهداف وتكون مخرجاتها حزمة من الوسائل والإجراءات في ميادين التقنية والقانون وإدارة النظم التقنية، وبوصفها عملية تكاملية، فإنها محكومة باستراتيجية تحدد عناصر الحماية ونطاقها، لهذا فإن من الخطأ القاتل مجرد الاعتقاد أن استخدام بعض التقنيات التي تحمي البيانات الشخصية قد حقق حماية للخصوصية، ومن الاعتقادات الخاطئة أيضا أن مجرد التزام جهات جمع البيانات باحترام الخصوصية يحقق الحماية أو يحقق مساءلتها إن حصل إخلال، والخطأ الأكثر خطورة إغفال أهمية الحماية القانونية الشمولية وتكاملها مع الحماية التقنية والخطوات التنظيمية.

- ويثور التساؤل هنا عن كيفية تحقيق التوازن بين الحق في خصوصية البيانات والاستفادة من إعلانها **(المطلب الأول)**.
- وأيضاً هل الحفاظ على خصوصية البيانات مسؤولية المستهلك وحده أو مسؤولية قطاع الأعمال؟ **(المطلب الثاني)**.
- وكيفية الموازنة بين الحماية ومعالجة البيانات بأنواعها المختلفة**(المطلب الثالث)**.

المطلب الأول

التناقض بين الحق في الحماية والاستفادة من إعلان البيانات الشخصية

إن الإنترنت كما هو معلوم واسطة اتصالات جديدة، وموقع وموضع جديد للجهات الحكومية ومؤسسات الأعمال والهيئات الاجتماعية في البيئة العالمية، وبسبب عدم مركزيتها وكونها مفتوحة، وذات طبيعة تفاعلية، فإنها مثلت أول وسيلة إلكترونية تسمح لكل مستخدم نشر ما يشاء والتدخل فيما يريد من أنشطة تجارية، فالمستخدمين يمكنهم الوصول وإنشاء الاتصالات مع جهات عديدة بغض النظر عن الحدود الجغرافية وعن المعيقات الاجتماعية والسياسية، وهي واسطة غير متناهية في القدرة والحجم وأقل كلفة بالنسبة لإيصال الخدمات الحكومية والاجتماعية والمعرفية، في شتى مجالات النشاط الإنساني، وحيث نما (الويب) بسبب دعمه الكتابة والصوت والفيديو والصورة، فقد أصبح (الويب) مجتمعا وملتقى العالم الافتراضي، وأتاح التفاعل (وجها لوجه) في عالم بلا حدود.

وقد ثار التساؤل حول ما إذا كانت ستتحقق ديمقراطية الإنترنت فعلا، فهي بمفاهيمها الاجتماعية والسياسية والتقنية تتضمن عناصر الديمقراطية، ومن هنا فإن الحكومات التي تشجع انتشار الإنترنت تخاف في الوقت نفسه مخاطرها وتهديدها لسلطاتها التقليدية. والقطاع الخاص يشهد ويتعامل مع الفرص الاقتصادية للإنترنت، لكن مخاطر المنافسة المضادة أو غير المشروعة تظل قائمة أكثر من مخاطرها في البيئة المادية، والمستخدمون لا ينقلون فقط تفاعلهم الاجتماعي الإيجابي على الإنترنت، ولكن أيضا احتمالات السلوكيات غير المقبولة وحالات عدم التقبل الاجتماعي.

فتمكن تقنية المعلومات الجديدة تخزين واسترجاع وتحليل كميات هائلة من البيانات الشخصية التي يتم تجميعها من قبل المؤسسات والدوائر

والـوكالات الحكوميـة ومـن قبـل الـشركات الخاصـة، ويعـود الفضـل لهـذا إلى مقـدرة الحوسـبة الرخيصـة، وأكـثر مـن هـذا فإنـه يمكـن مقارنـة المعلومـات المخزونـة في ملـف بمعلومـات في قاعـدة بيانـات أخـرى، ويمكـن نقلها عبر البلد في ثـوان وبتكاليـف منخفضة نسـبيا، "إن هـذا بوضـوح يكشـف إلى أي مـدى يمكـن أن يكـون تهديـد الخصوصيـة ".

وتتزايـد مخاطـر التقنيـات الحديثـة عـلى حمايـة الخصوصيـة، كتقنيـات رقابـة (كامـيرات) الفيديـو، وبطاقـات الهويـة والتعريـف الإلكترونيـة، وقواعـد البيانـات الشـخصية، ووسـائل اعـتراض ورقابـة البريـد والاتصـالات، ورقابـة بيئـة العمـل وغيرهـا.[1]

والحقيقـة أن اسـتخدام وسـائل التقنيـة العاليـة في ميـدان جمـع ومعالجـة البيانـات الشـخصية مـن قبـل الدولـة أو القطـاع الخـاص، قـد عمـق التناقضـات الحـادة التـي بـرزت منـذ القـدم بـين حـق الأفـراد في الحيـاة الخاصـة، وموجبـات اطـلاع عـلى شـؤون الأفـراد. وتتمثـل هـذه التناقضـات، بمعـالم أربعـة رئيسـة:[2]

أولا: التناقـض بـين حـق الحيـاة الخاصـة وحـق الدولـة في الاطـلاع عـلى شـؤون الأفـراد، والـذي عمقـه تزايـد تدخـل الدولـة في شـؤون الأفـراد، وليـس المـراد بهـذا التدخـل الاطـلاع عـلى معلومـات معينـة عـن الأفـراد لتنظيـم الحيـاة الاجتماعيـة عـلى نحـو أفضـل، كالاحتفـاظ بسـجلات الـولادات والـزواج والوفيـات والإحصـاءات وغيرهـا،

---

(1) أحمد جاد منصور،ضمانات الحق في حرمة الحياة الخاصة،المنظمة العربية للتنمية الإدارية،2013، ص 53

(2) محمود عبد الرحمن محمد،نطاق الحق في الحياة الخاصة،دار النهضة العربية،1995 ص 23 - 53 وراجع في نفس الموضوع عصام أحمد البهجي،حماية الحق في الحياة الخاصة في ضوءحقوق الإنسان،الدار العربية للنشر والتوزيع،2000

See Alos David Banisar،The Right to Information and Privacy: Balancing Rights and Managing Conflicts، Global Campaign for Free Expression World Bank Institute Governance Working Paper،، 2011 P10

بـل اسـتخدام الدولـة للمعلومـات الشـخصية الخاصـة بالفـرد لأغـراض تتناقـض مـع صونهـا واحترامهـا.

ثانيـا: التناقـض بـين حـق الفـرد في الاحتفـاظ بسريتـه، ومصلحتـه في كشـف حياته الخاصـة ليتمتـع بثـمار هـذا الكشـف. ورغـم أن هـذا التناقـض للوهلـة الأولى غـير متحقـق، باعتبـار أن الاحتفـاظ بالسريـة حـق، والكشـف الطوعـي عـن هـذه السريـة حـق أيضـا، فـإن احتـمال اسـتغلال المعلومات المعطـاة طوعـا لأغـراض غـير التـي أعطيـت لأجلهـا يمثـل انتهـاكا لحرمـة الفـرد وسريتـه.

ثالثـا: التناقـض بـين الحيـاة الخاصـة، والحـق في جمـع المعلومـات لغايـات البحث العلمـي، أو حريـة البحـث العلمي.

رابعـا: التناقـض بـين الحـق في الحيـاة الخاصـة وبـين حريـة الصحافـة وتبـادل المعلومـات (الحريـة الإعلاميـة).

هـذه التناقضـات بـرزت منـذ القـدم بـين حـق الفـرد في حمايـة حياتـه الخاصـة، وبـين موجبـات الاطـلاع عـلى شـؤون الفـرد، بمـا فيهـا تلـك التـي تقـع ضمـن نطـاق حياته الخاصـة. وإذا كانـت الجهـود التنظيميـة، الإداريـة والتشريعية، سـعت إلى إقامـة التوازن بـين هـذه الحقـوق المتعارضـة فـإن اسـتخدام التقنيـة في ميدان جمـع ومعالجـة البيانات الشـخصية، قـد خلـق واقعـا صعبـا هـدد هـذا التوازن مـن جهة وعمـق حـدة التناقضات المشـار إليهـا مـن جهـة أخرى.

وكذلـك التضـارب بـين حريـة التعبـير وخصوصيـة البيانـات، إن مسـألة التضـارب بـين حريـة التعبـير وخصوصيـة البيانـات عـلى الإنترنـت أكـثر تعقيـداً وتنوعـاً مـن تلـك التضاربـات الناجمـة عـن أثـر ضعـف وسـائل الحمايـة الخاصـة بسريـة وخصوصيـة البيانـات عـلى حريـة التعبـير، وعـلى ذلـك فإنـه فيـما أن الأخـير عـادة مـا ينطـوي عـلى تدخـلات واضحـة مـع سريـة البيانـات، والتـي عـادة مـا بذلـت جميـع الجهـود اللازمـة لتبريرهـا بسـبب احتياجـات تنفيـذ القانـون الضروريـة، ومـن ثـم

تصبح مسألة ما هو الذي يشكل سرية البيانات أمراً في غاية الحيوية والأهمية، لقد رفضت المحاكم الدولية المحلية والدولية تقديم تعريف واضح عن السرية، برغم أن الاتجاه الذي اتخذته المحاكم في الولايات المتحدة الأمريكية، والذي يتضمن عناصر شكلية (التوقع الفعلي لسرية البيانات) والموضوعية)التوقعات المعقولة لسرية البيانات(، لديه من المبررات والمسوغات اللازمة للتوصية به.[1]

وأصبح نطاق مفهوم خصوصية البيانات أمراً مهماً للغاية في بعض الحالات التي تشمل حرية التعبير، على سبيل المثال، هل يوجد لدى وزير الدفاع توقعات معقولة عن مدى خصوصية البيانات عندما يكون مدعواً على العشاء في مطعم، ولكن مع موزع أسلحة أجنبي؟ ماذا لو دُعي رئيس وزراء لحفل زفاف شخصية مشهورة؟

مما لا شك فيه أن هذا السؤال يمكن الإجابة عنه بشكل مختلف في دول مختلفة، مع وجود تداعيات مهمة بالنسبة لوسائل الإعلام التي تسعى لسبق صحفي عن هذه الأنشطة. وينبغي أن يفهم هذا الموضوع أيضاً في ضوء الإطار الرئيس للتحديات التي تواجه حماية سرية البيانات في عالم الإنترنت والخدمات المقدمة عبر الإنترنت، وأنماط الاستجابات التنظيمية والقانونية التي أفرزتها، وفيما أوضح هذا التقرير، فإن هناك تحديات ضخمة أمام تنظيم سرية البيانات[2].

إن استخدام الحواسيب في ميدان جمع ومعالجة البيانات الشخصية المتصلة بالحياة الخاصة للأفراد خلف آثارا إيجابية عريضة، لا يستطيع أحد

(1) يوسف الشيخ يوسف، حماية الحق في حرمة الأحاديث الخاصة، دار الفكر العربي،2001 ص 23.

(2) Davis، Darren and Brian Silver. "Civil Liberties vs. Security: Public Opinion in the Context of the Terrorist Attacks on America." American Journal of Political Science. Vol. 48. 1. 2004. P 5

إنكارها خاصة في مجال تنظيم الدولة لشؤون الأفراد الاقتصادية والاجتماعية والعلمية، وغيرها، وهذا ما أوجد في الحقيقة ما يعرف ببنوك المعلومات (بالانجليزية Data Bank وبالفرنسية Les Banques de Donness) وبنوك المعلومات قد تكون مقصورة على بيانات ومعلومات تتصل بقطاع بعينه، كبنوك المعلومات القانونية مثلا، أو قد تكون شاملة لمختلف الشؤون والقطاعات، وقد تكون مهيأة للاستخدام على المستوى الوطني العام كمراكز وبنوك المعلومات الوطنية أو المستخدمة على نحو خاص، كمراكز وبنوك معلومات الشركات المالية والبنوك وقد تكون كذلك مهيأة للاستخدام الإقليمي أو الدولي. [1]

وكما سبق الإشارة إلى أن بنوك المعلومات، هي:" تكوين قاعدة بيانات تفيد موضوعا معينا وتهدف لخدمة غرض معين، ومعالجتها بواسطة أجهزة الحاسبات الإلكترونية (الحواسيب) لإخراجها في صورة معلومات تفيد مستخدمين مختلفين في أغراض معينة "ومن الوجهة الفنية، يقصد بها" العمليات المختلفة للحاسب الإلكتروني أو الكمبيوتر، من تسجيل وتصنيف البيانات.[2]

وبفعل الكفاءة العالية لوسائل التقنية والإمكانات غير المحدودة في مجال تحليل واسترجاع المعلومات، اتجهت جميع دول العالم بمختلف هيئاتها ومؤسساتها إلى إنشاء قواعد البيانات لتنظيم عملها، واتسع على نحو كبير استخدام الحواسيب لجمع وتخزين ومعالجة البيانات الشخصية لأغراض متعددة فيما يعرف ببنوك ومراكز المعلومات الوطنية، ومع تلمس المجتمعات لإيجابيات استخدام الحواسيب في هذا المضمار ظهر بشكل متسارع أيضا، الشعور بمخاطر تقنية المعلومات وتهديدها للخصوصية.[3]

---

(1) محمد على فارس الزغبي، الحماية القانونية لقواعد البيانات، منشأه المعارف،2010 ص 100 - 103.

(2) المرجع السابق،ص 30.

(3) Brennan، William. "The Quest to Develop Jurisprudence of Civil

هـذا الشـعور نما وتطـور بفعـل الحـالات الواقعيـة للاسـتخدام غـير المـشروع للبيانـات الشـخصية واتسـاع دائـرة الاعتـداء عـلى حـق الأفـراد في الحيـاة الخاصـة، مـما حـرك الجهـود الدوليـة والإقليميـة والوطنيـة - التـي نعـرض لهـا تاليـا - لإيجـاد مبـادئ وقواعـد مـن شـأن مراعاتهـا حمايـة الحـق في الحيـاة الخاصة، وبالـضرورة إيجـاد التوازن بـين حاجـات المجتمـع لجمـع وتخزيـن ومعالجـة البيانـات الشـخصية، وكفالـة حمايـة هـذه البيانـات مـن مخاطـر الاسـتخدام غـير المـشروع لتقنيـات معالجتهـا.[1]

وإذا كانـت الجهـود الدوليـة والاتجـاه نحـو الحمايـة التشريعيـة للحيـاة الخاصـة عمومـا، وحمايتهـا مـن مخاطـر اسـتخدام الحواسـيب وبنـوك المعلومات عـلى نحو خاص، تمثـل المسـلك الصائـب في مواجهـة الأثـر السـلبي للتقنيـة عـلى الحيـاة الخاصـة، فإن هذا المسـلك قـد رافقـه اتجـاه متشـائم لاسـتخدام التقنيـة في معالجـة البيانـات الشـخصية. فالتوسـع الهائـل لاسـتخدام الحواسـيب قـد أثـار المخـاوف مـن إمكانيـة انتهـاك الحيـاة الخاصـة، وذلـك لأن المعلومـات المتعلقـة بجميـع جوانـب حيـاة الفـرد الشـخصية، كالوضـع الصحـي والأنشـطة الاجتماعيـة والماليـة والسـلوك والآراء السياسـية، يمكـن جمعهـا وخزنهـا لفـترة غـير محـددة، كـما يمكـن الرجـوع إليهـا جميعـا بمنتهـى السرعـة والسـهولة.

ومـع الزيـادة في تدفـق المعلومـات التـي تحدثهـا الحواسـيب، تضعـف قـدرة الفـرد عـلى التحكـم في تدفـق المعلومـات عنـه، وعمليـة إعـداد المعلومـات ومعالجتهـا عـبر أجهـزة الحواسـيب واسـتخلاص النتائـج منهـا يزيـد - كـما يـرى

Liberties in Times of Security." 2007. Available at http://www.brennancenter.org/resources/downloads/nation_security_brennan.pdf.See also. Willard Marriott Library. Japanese - Americans Internment Camps During World War II. 16 April 2007 http://www.lib.utah.edu/spc/photo/90669066/.htm.

(1) Adams، Helen. Privacy in the 21st Century. Connecticut: Libraries Unlimited American Library Association، 2005.P72

الكثيرون في الغرب [1] - خطر التقنوقراطية، لأن الاعتماد على جهاز لعقلنة الخيارات في الإنفاق والتخطيط والتعليم والسياسة وما أشبه يعرض مفهوم الديمقراطية للخطر والسبب هو أن الخيارات المتخذة وفقا لمبادئ حسابية تستبعد السيكولوجية الاجتماعية، وحتى إذا أدرجت هذه الاعتبارات، كعامل مساعد في المعلومات التي يغذي بها الحاسوب، فهي لن تكون إلا ذات أهمية ثانوية.

يقول Robert M.Bowie: "إن التقنوقراطية، وهي تملك الكمبيوترات قد تصبح على درجة بالغة من القوة بحيث تحبس الحياة الخاصة داخل حدود ضيقة، وتكيف حياة الفرد وأسرته بهذه الأجهزة في اللحظة التي تكون لها في ذلك مصلحة اقتصادية أو اجتماعية [2]، وبذلك يصبح الإنسان معاملا كالأرقام، بكمبيوتر مسلوب الإرادة في اتخاذ قراراته بوعي واستغلال، ومفرغا أخيرا من شخصيته "، إن ما يهدد الجنس البشري ليس حربا نووية، بل جهاز كمبيوتر مستقل".

إن هذه النظرة - كما يظهر لنا، نظرة متشائمة من شيوع استخدام الحواسيب وأثرها على تهديد الخصوصية، وهي وان كانت نظرة تبدو مبالغا فيها، إلا أنها تعكس حجم التخوف من الاستخدام غير المشروع للتقنية، وتحديدا الحواسيب، في كل ما من شأنه تهديد الحق في الحياة الخاصة، ويمكننا فيما يلي إجمال المعالم الرئيسة لمخاطر الحواسيب وبنوك المعلومات على الحق في الحياة الخاصة بما يلي:

أولا: "إن الكثير من المؤسسات الكبرى والشركات الحكومية الخاصة، تجمع عن الأفراد بيانات عديدة ومفصلة تتعلق بالوضع المادي أو الصحي

---

(1) الأمم المتحدة - أعمال الأمم المتحدة في ميدان حقوق الإنسان - المجلد الأول. منشورات هيئة الأمم المتحدة (رقم المبيع 15564 - 89 GE نيويورك، 1990.

(2) د. صالح جواد كاظم،" التكنولوجيا الحديثة والسرية الشخصية"، الطبعة الأولى، بغداد، 1991ص267.

أو التعليمي أو العائلي أو العادات الاجتماعية أو العمل..الخ، وتستخدم الحاسبات وشبكات الاتصال في خزنها ومعالجتها وتحليلها والربط بينها واسترجاعها ومقارنتها ونقلها، وهو ما يجعل فرص الوصول إلى هذه البيانات على نحو غير مأذون به أو بطريق التحايل أكثر من ذي قبل، ويفتح مجالا أوسع لإساءة استخدامها أو توجيهها توجيها منحرفا أو خاطئا أو مراقبة الأفراد وتعرية خصوصياتهم أو الحكم عليهم حكما خفيا من واقع سجلات البيانات الشخصية المخزنة ".

على سبيل المثال، فإن حكومة الولايات المتحدة وفق دراسات 1990 جمعت 4 بليون سجل مختلف حول الأمريكيين، بمعدل (17) بندا لكل رجل وامرأة وطفل، ومصلحة الضريبة (IRS) في الولايات المتحدة تمتلك سجلات الضرائب لحوالي (100) مليون أمريكي على حواسيبها، وتملك الوكالات الفيدرالية - عدا البنتاغون - ثلاث شبكات اتصالات منفصلة تغطي كل الولايات المتحدة الأمريكية لنقل وتبادل البيانات.

ولنتخيل أن هذه الأرقام كانت في ظل غياب الإنترنت وفي ظل بدايات الاعتماد على التشبيك الواسع النطاق، وقبل عشر سنوات، ثانيا: إن شيوع (النقل الرقمي) للبيانات خلق مشكلة أمنية وطنية، إذ سهل استراق السمع والتجسس الإلكتروني.

ففي مجال نقل البيانات "تتبدى المخاطر المهددة للخصوصية في عدم قدرة شبكات الاتصال على توفير الأمان المطلق أو الكامل لسرية ما ينقل عبرها من بيانات وإمكانية استخدام الشبكات في الحصول بصورة غير مشروعة، عن بعد على المعلومات"، ولم تحل وسائل الأمان التقنية من الحماية من هذه المخاطر[1] وفي الأعوام من 1993 وحتى 2000 نشط البيت الأبيض

---

(1) فعلى سبيل المثال، وجه الرئيس الأمريكي ريغان عام 1984 إلى شبكة (NEA) الدعوة للبحث عن طرق تنتج شبكات هاتفية آمنة بشكل أكبر للاتصالات الخاصة بالمعلومات الحكومية الحساسة، إلا أن تكاليف تركيب هواتف آمنة وبمساعدة نبائط (الخلط) =

الأمريكي والهيئات المتخصصة التي أنشأها لهذا الغرض في توجيه جهات التقنية إلى العمل الجاد على خلق تقنيات أمان كافية للحفاظ على السرية الخصوصية، وبالرغم من التقدم الكبير على هذا الصعيد فإن أحدث تقارير الخصوصية تشير إلى أنه لم تزل حياة الأفراد وأسرارهم في بيئة النقل الرقمي معرضة للاعتداء في ظل عدم تكامل حلقات الحماية(التنظيمية والتقنية والقانونية).

ثانيا: إن أكثر معالم خطر بنوك المعلومات على الحياة الخاصة، ما يمكن أن تحويه من بيانات غير دقيقة أو معلومات غير كاملة لم يجر تعديلها بما يكفل إكمالها وتصويبها. فعلى سبيل المثال، كلف مكتب تقييم التقنية في الولايات المتحدة (OTA) في عام 1981 الدكتور (لوردن)، وهو عالم في مجال الجريمة، بإجراء دراسة حول قيمة بيانات التاريخ الإجرامي التي تحويها ملفات (FBI - وكالة الشرطة الفيدرالية) وملفات وكالة شرطة ولاية نيويورك، وقد وجد أن نسبة عالية من البيانات كانت غير كاملة وغير دقيقة ومبهمة، ويتضمن العديد منها اعتقالات وتقصيات لم تؤد إلى إدانة، أو أنها متعلقة بجنح بسيطة تمت في الماضي القديم، وأظهرت دراسات أخرى أن أصحاب العمل لم يوظفوا في الغالب مثل هؤلاء الأشخاص لسجلاتهم الإجرامية غير الدقيقة، واعترفت أربع من خمس ولايات أمريكية تم الاتصال معها بواسطة مكتب تقييم التقنية (OTA) أنها لم تتأكد أبدا من دقة البيانات في ملفاتها، أو أنها لم تقم باستماع نوعي منتظم.[1]

=تعتبر عالية، وقد كشفت شركة (BT بريتيش تيليكوم) في المملكة المتحدة النقاب في عام 1986 عن نبيطة على شكل شريحة تقوم بالتشفير وتعمل على خلط المعلومات بما يتيح التمويه قبل أن يتم إرسالها على خطوط المواصلات، لكن الواقع العملي كشف عن استخدام وسائل تقنية تبطل مفعول مثل هذه النبائط الإلكترونية.

(1) Michael، J، "Privacy and human Rights"، An international and comparative study with special reference of development in information technology، (1994) P.72

ثالثا: إن المعلومات الشخصية التي كانت فيما قبل منعزلة متفرقة، والتوصل إليها صعب متعذر، تصبح في بنوك المعلومات مجمعة متوافرة متكاملة سهلة المنال، متاح أكثر من ذي قبل استخدامها في أغراض الرقابة على الأفراد. وهكذا تبدو صائبة مقولة آرثر ميللر: إن الحاسب بشراهته التي لا تشبع للمعلومات، والسمعة التي ذاعت حول عدم وقوعه في الخطأ وذاكرته التي لا يمكن لما يختزن فيها أن ينسى أو ينمحي، قد تصبح المركز العصبي (Centre Nerveax) لنظام رقابي يحول المجتمع إلى عالم شفاف ترقد فيه عارية بيوتنا ومعاملاتنا المالية، واجتماعاتنا وحالتنا العقلية والجسمانية لأي مشاهد عابر".

رابعاً: إن تكامل عناصر الحوسبة مع الاتصالات والوسائط المتعددة أتاح وسائل رقابة متطورة سمعية ومرئية ومقروءة، إضافة إلى برمجيات التتبع وجمع المعلومات آليا، كما أتاح الإنترنت - واسطة هذه العناصر جميعا - القدرة العالية لا على جمع المعلومات فقط، بل معالجتها عبر تقنيات الذكاء الصناعي التي تتمتع بها الخوادم (أنظمة الكمبيوتر المستضيفة وأنظمة مزودي الخدمات) والتي تتوفر أيضا لدى محركات البحث وبرمجيات تحليل الاستخدام والتصرفات على الشبكة، بحيث لا يستغرب معها أن الشخص عندما يتصل بأحد مواقع المعلومات البحثية في هذه الأيام يجد أمامه المواقع التي كان يفكر في دخولها والتوصل بها، كما لا يستغرب مستخدم الإنترنت أن ترده رسائل بريد الكتروني تسويقية من جهات لم يتصل بها تغطي ميوله ورغباته.

إن بدء مشكلات الكمبيوتر في الستينات ترافق مع الحديث - في العديد من الدول الغربية - عن مخاطر جمع وتخزين وتبادل ونقل البيانات الشخصية، ومخاطر تكنولوجيا المعلومات في ميدان المساس بالخصوصية والحريات العامة، وانتشر الحديث عن الخطر الكبير التي يتهدد الحرية الشخصية بسبب المقدرة المتقدمة لنظم المعالجة الإلكترونية على كشف والوصول إلى المعلومات المتعلقة بالأفراد واستغلالها في غير الأغراض التي تجمع من أجلها.

وخلال الثمانينات تغير الواقع التكنولوجي فيما يتعلق بالجهات التي تملك وتسيطر على نظم الكمبيوتر وكان ذلك بسبب إطلاق الحواسيب الشخصية وانتشارها، وأصبح من الواضح أن حماية الخصوصية يتعين أن تمتد إلى الكمبيوترات الخاصة، وأن يتم إحداث توازن ما بين الحق في الخصوصية أو الحق في الحياة الخاصة وبين الحق في الوصول إلى المعلومات، هذا التغير في الواقع التكنولوجي عكس نفسه على حقل الحماية القانونية في الخصوصية بأبعادها التنظيمية والمدنية والجزائية وبدأت تكثر الأحاديث بشأن دعاوى الاستخدام غير المشروع للمعلومات وللوثائق الشخصية، وظهرت أحداث شهيرة في حقل الاعتداء على البيانات الخاصة من بينها - على سبيل المثال – الذي حدث في جنوب إفريقيا حيث أمكن للمعتدين الوصول إلى الأشرطة التي خزنت عليها المعلومات الخاصة بمصابي أمراض الإيدز وفحوصاتهم، وقد تم تسريب هذه المعلومات الخاصة والسرية إلى جهات عديدة.

ومن الحوادث الشهيرة الأخرى حادثة حصلت عام 1989 عندما تمكن أحد كبار موظفي أحد البنوك السويسرية بمساعدة سلطات الضرائب الفرنسية بأن سرب إليها شريطا يحتوي على أرصدة عدد من الزبائن، وقد تكرر مثل هذا الحادث في ألمانيا أيضا.

وقد أظهرت القضايا التي حصلت ما بين عامي 96 - 97 في الحقل المصرفي أن الوصول إلى البيانات الشخصية ارتبط في الغالب بأنشطة الابتزاز التي غالبا ما تتعلق بالتحايل على الضريبة من قبل زبائن البنوك[1].

وفي عام 1986 اتهمت شركة IBM بأن نظام الأمن التي تنتجه المسمى RACF يستخدم للرقابة على الموظفين داخل المنشآت،[2] وفي عام

---

(1) ulrich sieber، جرائم تقنية المعلومات، بالفرنسية والألمانية 1994 ص67 Computer - related crime

(2) A. Snell، "IT security gets personal." Management & Careers Ethica Publishing، 2007 P 34

1994 أيضا وفي ألمانيا أثير جدل واسع حول حق دائرة التأمينات الصحية بنقل البيانات الشخصية إلى شركات خارجية، وشبيه بهذا الجدل ما يثور الآن بشأن مدى أحقية شركات تزويد الإنترنت والتلفونات الكشف عن معلومات الزبائن لجهات أخرى.

لقد ارتكبت العديد من جهات الرقابة أنشطة إساءة استخدام البيانات الخاصة حتى في أكثر الدول المتقدمة، وكان الهدف من وراء هذه الاعتداءات في الغالب سياسيا أو اقتصاديا، لهذا كانت البيانات المستهدفة هي بيانات المعارضة السياسية والصحفيين وناشطي حقوق الإنسان، وهو ما اقتضى تزايد النشاط الدولي في حقل حماية الخصوصية من أنشطة الرقابة الإلكترونية ELETRONIC SURVEILLAN[1].[2]

---

(1) J. Hollwitz، "The Development of a Structured Ethical Integrity Interview for Pre - Employment Screening." The Journal of Business Communication (1997): 203 - 219.

(2) Electronic Surveillan:Observing or listening to persons، places، or activities—usually in a secretive or unobtrusive manner—with the aid of electronic devices such as cameras، microphones، tape recorders، or wire taps. The objective of electronic surveillance when used in law enforcement is to gather evidence of a crime or to accumulate intelligence about suspected criminal activity. Corporations use electronic surveillance to maintain the security of their buildings and grounds or to gather information about competitors. Electronic surveillance permeates almost every aspect of life in the United States. In the public sector، the president، Congress، judiciary، military، and law enforcement all use some form of this technology. In the private sector، business competitors، convenience stores، shopping centers، apartment buildings، parking facilities، hospitals، banks، employers، and spouses have employed various methods of electronic eavesdropping. Litigation has even arisen from covert surveillance of restrooms.Three types of electronic surveillance are most prevalent: wire tapping، bugging، and videotaping. Wire tapping intercepts telephone calls and telegraph messages by physically penetrating the wire circuitry. Someone must

وعلى الرغم من ذلك فإن هذه النصوص التقليدية لحماية شرف الإنسان وحياته الخاصة لا تغطي إلا جانبا من الحقوق الشخصية وبعيدة عن حمايته من مخاطر جمع وتخزين والوصول إلى مقارنة واختيار وسيلة نقل المعلومات في بيئة الوسائل التقنية الجديدة، هذه المخاطر الجديدة التي تستهدف الخصوصية دفعت العديد من الدول لوضع تشريعات ابتداء من عقد السبعينات من القرن المنصرم، تتضمن قواعد إدارية ومدنية وجنائية من أجل حماية الخصوصية وتوصف بأنها تشريعات السرية، وليست فقط مجرد تشريعات تحمي من أفعال مادية تطال الشرف الاعتبار والحياة الخاصة.

كما أن هذه المخاطر وما يتفرع عنها من مخاطر أخرى - كتلك الناتجة عن معالجة البيانات في شبكات الحواسيب المربوطة ببعضها البعض، والتي تتيح تبادل المعلومات بين المراكز المتباعدة والمختلفة من حيث أغراض تخزين البيانات بها - نقول إن هذه المخاطر كانت محل اهتمام دولي وإقليمي ووطني أفرز قواعد ومبادئ تتفق وحجم هذه المخاطر، كوجوب مراعاة الدقة في جمع البيانات، وكفالة صحتها وسلامتها، واتخاذ تدابير أمنية لمعالجتها وخزنها ونقلها، وإقرار مبدأ حق المشاركة الفردية في تعديل وتصحيح وطلب إلغاء

---

actually "tap" into telephone or telegraph wires to accomplish this type of surveillance. Bugging is accomplished without the aid of telephone wires، usually by placing a small microphone or other listening device in one location to transmit conversations to a nearby receiver and recorder. Video surveillance is performed by conspicuous or hidden cameras that transmit and record visual images that may be watched simultaneously or reviewed later on tape. Electronic eavesdropping serves several purposes: (1) enhancement of security for persons and property; (2) detection and prevention of criminal، wrongful، or impermissible activity; and (3) interception، protection، or appropriation of valuable، useful، scandalous، embarrassing، and discrediting information. The law attempts to strike a balance between the need for electronic surveillance and the privacy interests of those affected.

البيانات، ووجوب تحديد الغرض من جمعها ومدة استخدامها، وإقرار مبدأ مسؤولية القائمين على وظائف بنوك المعلومات لأي تجاوز أو مخالفة للمبادئ الموضوعية والشكلية في جمع ومعالجة وتخزين ونقل البيانات الشخصية، وهذه المبادئ أكدت عليها أيضا تشريعات حماية الحياة الخاصة، ونتناول فيما يلي الاتجاهات الدولية والإقليمية لحماية الخصوصية كما نستعرض الإطار العام للتدابير التشريعية في هذا الحقل من حيث بيان مداها ومحتواها العام. [1]

وثمة خمسة مبادئ أساسية تحتم الممارسات العادلة والمقبولة أو النزيهة في نطاق خصوصية المعلومات أو حماية البيانات الشخصية في البيئة الرقمية، هذه المبادئ هي:

الإبلاغ / الإخطار Notice:

ويراد بهذا المبدأ أن مستخدمي المواقع يتعين إبلاغهم من قبل مزود الخدمة أو الموقع ما إذا كان الموقع أو مقتضيات الخدمة ينطويان على جمع بيانات شخصية وإلى أي مدى تجمع هذه البيانات وتستخدم.

الاختيار Choice:

ويوجب هذا المبدأ التزام الشركات صاحبة المواقع أو مزودي الخدمة بتوفير خيار للمستخدم بشأن استخدام بياناته فيما يتجاوز غرض جمعها الابتدائي.

الوصول للبيانات Access:

ويوجب هذا المبدأ قدرة المستخدمين للوصول إلى بياناتهم والتثبت من صحتها وتحديثها.

---

(1) انتصار عباس إبراهيم. أثر وسائل الاتصال في خدمات المكتبات ومراكز المعلومات. الخرطوم: جامعة النيلين، 2005 م. - ص 8 (رسالة ماجستير).

الأمن Security:

ويتعلق هذا المبدأ بمسؤوليات جهات جمع البيانات (المواقع ومزودي الخدمة) بشأن معايير الأمن المتعين تطبيقها لضمان سرية البيانات، وسلامة الاستخدام وحظر الوصول غير المصرح به لهذه البيانات، وتتضمن من ضمن ما تتضمن وسائل كلمات السر والتشفير وغيرها من وسائل أمن المعلومات التي عرضنا لها تفصيلا في الجزء الأول من هذا الدليل.

تطبيق القانون Enforcement:

ويتعلق هذا المبدأ بالآليات المناسبة المتعين اعتمادها لفرض الجزاءات على الجهات غير المتوافقة مع المبادئ المتقدمة وما يتصل بها من الممارسات النزيهة بشأن جمع البيانات الشخصية في البيئة الرقمية.[1]

وفي المقابل فإن هذه المبادئ الخمسة المقيدة لتعامل جهات المواقع مع البيانات الشخصية، يتعين أن لا تنتقص من سمات مجتمع الإنترنت الديمقراطي، وهي في حقيقتها لا تتعارض مع هذه السمات لأن موجبات ديمقراطية الإنترنت عدم التغول على حقوق المستخدمين، ولكن وحتى تكون عمليات الاستخدام في منأى من التشدد، يعمل بالتوازي مع هذه المبادئ، مبدأ رضا وموافقة المستخدم إلى جانب الاستثناءات المقررة بموجب معايير تزويد الخدمة التي تتيح قدرا من الحرية لجهات جمع البيانات بموجب ما هو مقرر في نظم مسؤولياتها القانونية أو مدونات السلوك التي تحكمها. مع ضوابط محددة لضمان صحة وسلامة الرضا وضبط الاستثناءات أو ما يمكن تسميته الممارسات المسموح بها لجهات تزويد الخدمة وإدارة المواقع.

---

(1) Fred H. Cate،FAIR INFORMATION PRACTICE PRINCIPLES forthcoming in Consumer Protection in the Age of the 'Information Economy 2005 P 16 available http://www.informationpolicycentre.com/files/Uploads/Documents/Centre/Failure_of_Fair_Information_Practice_Principles.pdf

إن أخطر ما يلحظه الباحث، ليس مجرد غياب هذه المبادئ في قطاع عريض من مواقع الإنترنت، بل عدم فعاليتها رغم التزام المواقع بها بسبب ما تعتمده هذه المواقع من وسائل تجعلها غير ذات قيمة، فعندما تكون سياسة الموقع المعلنة بموجب وثيقة (الخصوصية) على الموقع تتضمن التزامات تعكس هذه المبادئ، فإن هذه السياسات ذاتها تنطوي على استثناءات تحد من فعالية وموجبات مبادئ الحماية، وتسعى المواقع إلى بعض الممارسات التي لا تشجع على قراءة هذه السياسات وإدراك حدود الالتزامات والاستثناءات.

إن التوازن بين مجتمع الإنترنت الديمقراطي وموجبات حماية خصوصية المستخدمين يتحقق عن طريق المعيار المنضبط والمرن في ذات الوقت، معيار يكفل للمستخدم حماية بياناته الشخصية التي يصار لجمعها من المواقع ويتيح للمواقع تعاملا متناسبا مع أغراض وسمات الإنترنت وأغراض الموقع نفسه دون تشدد أو مغالاة. ويوضح الشكل 1 تاليا العناصر المتقدمة التي يتعين الموازنة بينها لدى صياغة هذا المعيار.

ومن المهم التأكيد في هذا المقام أن ما أوجبته بيئة المعلومات الرقمية من ضرورة توفر معايير متوازنة، كالمعيار الذي يوازن بين الحق في المعلومات والخصوصية، أو معيار التوازن بين موجبات تقييد أنشطة المساس بخصوصية المعلومات على الإنترنت وبين سماتها الديمقراطية، وما سيرد لاحقا من معايير أخرى، ترتبط أو تتصل جميعا، لا بتنظيم تقنية المعلومات فحسب، بل بالنظام القانوني لحماية المستخدم ونظام الممارسات التجارية العادلة والمشروعة في البيئة الإلكترونية، ويتصل هذان الموضوعان بدراسات التجارة والسوق وتحديدا الممارسات التجارية العادلة وحماية المستهلك.

ونخلص مما سبق إلى أن هذه المخاطر أثارت وتثير مسالة الأهمية الاستثنائية للحماية القانونية - إلى جانب الحماية التقنية - للبيانات الشخصية، ومن العوامل الرئيسة في الدفع نحو وجوب توفير حماية تشريعية وسن قوانين

في هـذا الحقـل، أنـه وقبـل اختـراع الكمبيوتـر، فـإن حمايـة هـؤلاء الأشـخاص كانـت تتـم بواسـطة النصـوص الجنائيـة التـي تحمـي الأسرار التقليديـة (كحمايـة الملفـات الطبيـة أو الأسرار المهنيـة بـين المحامـي والمـوكل).

المطلب الثاني

حماية خصوصية المعلومات، خيار قطاع الأعمال بقدر ما هو خيار المستخدم

ليس المستخدمون أو الأفراد هم من يهتمون بالخصوصية وحدهم، فمع ما أظهرته الدراسات المسحية في بيئة التجارة الإلكترونية من مخاطر عدم ثقة المستخدمين بالإنترنت بسبب الخصوصية، ظهر اهتمام عريض ومتزايد لدى قطاعات الأعمال[1].

وأصبح موضوع الخصوصية يؤخذ على محمل الجد، وأحيانا كعامل خطير يهدد أعمالها باعتبار أن عدم الثقة بالتجارة الإلكترونية بسبب الخشية على الخصوصية يمثل عائقا فاعلا لرواج التجارة الإلكترونية ذاتها في البيئة الرقمية.

ومن هنا ظهرت عشرات المبادرات للتنظيم الذاتي، وهو وسيلة قانونية تحظى باحترام المستهلكين والأفراد في العالم المتقدم، وتقوم على وضع مدونات سلوك ملزمة لقطاع معني، وفق رؤية هذا القطاع، فيلزم نفسه بما يخدمه، ومن قبيل تجارب التنظيم الذاتي في بيئة أعمال الإنترنت لتعزيز الخصوصية، مبادرة الثقة الإلكترونية (ترستي) TRUSTe[2]، ومجلس الأعمال لبرنامج الخصوصية على الخط Better Business Bureau's

(1) E. France، ‹Using Design to Deliver Privacy›، in One World، One Privacy، Towards an Electronic Citizenship، 22nd International Conference on Privacy and Personal Data Protection، Venice، 28 - 30 (September 2000)، p. 216; see also J. Borking، ‹Privacy Protecting Measures in IT Environment Necessary›، Information Management، 10،(1998)، pp. 6 - 11.

(2) http://www.truste.org

Online Privacy واتحاد الخصوصية على الخط Online Privacy Program[1]
Alliance [2]وغيرها.

ومع تزايد الشركات والجهات العاملة في بيئة الإنترنت وتزايد الجهات العاملة في حقل الأمن والخصوصية، نجد عشرات مبادرات التنظيم الذاتي، حتى أننا نجد الآن مواقع تروج لخدمات حماية الخصوصية تحت عناوين متعددة مثل: "privacy sensitivity" تشير إلى تقديم منتجات وخدمات تحمي الخصوصية والبيانات الحساسة.

كما أن كثيرا من الشركات التجارية عبر الإنترنت من غير العاملة في خدمات الأمن والخصوصية تستخدم شعارات الخصوصية نفسها في خططها التسويقية وموادها الإعلانية، وتتسابق في إظهار ما تستخدمه من تقنيات لحماية الخصوصية على الخط.

وهذه الجهود التي ساهمت في تعزيز الثقة بالإنترنت لدى كثيرين فإنها أيضا أثارت تساؤلات وتحديات كثيرة ليس آخرها التساؤل حول مدى ضمان الالتزام بقواعد التنظيم الذاتي في بيئة غير مركزية كالإنترنت لا تتحكم بها سلطة إجبار.

إن الحكومات تتجه أيضا، بل وتصارع من أجل إيجاد موضع ملائم لها في البيئة الإلكترونية، وقد انتهجت الكثير من الحكومات في تعاملها مع الإنترنت سياسة ترك الأمور إلى أن تتضح، وتبدو هذه السياسة أفضل ما تبدو لدى الولايات المتحدة، فهي قد أسست تعاملها مع الإنترنت على فكرة تنظيم السوق نفسه، ووضع كل الأطراف المتصارعة في موضع واحد علهم يصلون لاتفاق، ومع ذلك فإن سياسة التنظيم الذاتي وتنظيم السوق نفسه والحد الأدنى من التدخل لم تظل دون استثناءات بل وأحيانا ظهر توجه

(1) BBB Online http://www.bbbonline.org/privacy/fr_bd_ix.html P.12

(2) Online Privacy Alliance http://www.privacyalliance.org/ P.6

جديد نحو التحكمية والتنظيم الحكومي، مثال ذلك إقرار تشريعات في حقل الخصوصية، من بينها القانون الأمريكي بشأن حماية خصوصية الأطفال على الخط لعام 1998، وهذا يظهر توجها جديدا في مواجهة تحديات الخصوصية، ويبدو أن جهات التنظيم الخاص والذاتي للإنترنت نفسها هي التي تدفع نحو تبني قواعد وآليات لضمان تحكم المستخدمين بمعلوماتهم ولحماية الخصوصية.

المطلب الثالث

الموازنة بين الاندماج في العصر التكنولوجي و حماية معالجة البيانات الشخصية

بقدر ما تحتاج مجتمعات الغرب والدول المتقدمة إلى مزيد من الحلول القانونية لتساير ديناميكية إيقاع عصر المعلومات وهي تقود فتوحاته وتنتقل من بيئة إبداع إلى أخرى، فإن مجتمعاتنا العربية بأمس الحاجة إلى الانطلاق مما ملكت، وتعظيم ما تملك وهي تحاول أن تتلمس موطئ قدم في خضم التغيير المتسارع.

ولا يحقق وضوح البدايات الصحيحة غير إدراك البديهيات، ولا أبالغ عندما أقول: إننا نهدر البديهيات تحت ظن أننا نجيد المسائل المعقدة.

وأول بديهيات التعامل مع العصر الرقمي إدراك قيمة المعلومات وأهميتها والعمل على تكريس مفهوم حرية المعلومات وما يتصل بها من حقوق في منظومة قيمنا وقواعدنا الثقافية والتعليمية والأخلاقية والقانونية.

فالحق في المعلومات مفتاح الإبداع، وديدن التحول نحو مواطن النجاح، وليس المقصود إهدار القيود الموضوعية المتوائمة مع فكرة الحق ذاته والمبررة والمستمدة وجودها وسلامتها من المشروعية، وأول قيود المشروعية على حرية المعلومات موجبات حماية خصوصية الأفراد وحرمة حياتهم الخاصة وموجبات حماية بياناتهم الشخصية.

ومصدر الخطر الجديد على خصوصية الأفراد، نشأ جراء الاتساع العريض في استخدام تكنولوجيا الكمبيوتر computer technology، وعلى الرغم من أن استخدام الكمبيوتر في النشاط والخدمة في القطاعين العام والخاص لا يمثل من حيث الأصل اختلافا عن الوسائل التقليدية لحفظ ومعالجة البيانات، فإن ما يميز الكمبيوتر وتقنيات المعالجة المتطورة، وما قدمته من تسهيلات واسعة وما ظهر في نطاقها من قدرات عالية على أداء

أنشطة الجمع والخزن والمعالجة أظهر مصادر مستقلة للخطر، من ذلك الحجم الكبير للمعطيات، وتقنيات الخزن storage والاسترجاع retrieval، والقدرة على تبادل ونقل transmission المعطيات في نطاق واسع جدا قياسا بالطرق التقليدية، وعمليات التعديل والتدخل فيها، وفوق كل ذلك السرعة المذهلة والنطاق الواسع الذي تتم فيه كل هذه العمليات.

إلى جانب ما أتاحه الكمبيوتر من قدرة بناء بنوك المعلومات "data banks" لجمع قدر متزايد منها وبناء الشبكات التكاملية لجمع البيانات integrated networks of data collections على نحو أتاح النقل والتبادل والتزويد لكميات ضخمة من البيانات الشخصية في نطاق وعلى مساحة متزايدة وغير متناهية.

وعلى الرغم من أن قلة هم من ينكرون الفوائد الكبرى لتطبيقات المعالجة الإلكترونية للبيانات electronic data processing techniques، فإن القلق يتزايد بين الأفراد بشأن احتمالات الاستخدام غير الملائم لبياناتهم الشخصية في ضوء هذه الإمكانات التقنية المذهلة. وتحديدا الاستخدام غير المشروع للبيانات الشخصية المهمة والحساسة المخزنة إلكترونيا sensitive personal information stored electronically

وفي ضوء التطورات التقنية فإن إمكانية اتخاذ الأفراد وسائل وإجراءات لحماية حياتهم الخاصة وبياناتهم الشخصية من مخاطر تقنية الكمبيوتر تبدو صعبة قياسا بما يتطلبه الأمر لحماية خصوصيتهم من أنشطة الجمع والمعالجة والتسجيل التقليدية، والأخطر أن التقنية أتاحت أن تتحول البيانات التي تتعلق بالأفراد والتي قد تكون لوحدها وبذاتها غير ضارة، إلى بيانات قد تشكل تهديدا حقيقيا لخصوصية الأفراد وذلك بفعل ما أتاحته من مكنة الجمع والتحليل بين شتات البيانات المتفرقة وتحويلها إلى نوع من البيان التفصيلي أو البروفايل المتكامل عن حياة الفرد وأنشطته ومسلكياته.

إن القلق المتزايد من مخاطر تأثير التقنية على خصوصيات الأفراد،

وتحديدا في بيئة الإنترنت والتجارة الإلكترونية، يطرح التساؤل المهم حول الحماية التي نريدها، وحول فعالية برامجنا في حقل إشاعة التقنية وتوظيفها، ومدى قدرتها على الصمود وتحقيق الأهداف إذا لم تتحقق الثقة العالية بين مستخدم التقنية وبين أدواتها، وفي مقدمتها ثقته أن حياته لن تكون نهبا للآخرين، وأن أسراره لن تكون موضعا لعبث العابثين.

ونقطة الانطلاق الصحيحة نحو نظام قانوني يحاكي تحديات العصر ويدرأ مخاطر الآثار السلبية، هي القناعة أن الحق في المعلومات أصبح بحاجة إلى أكثر من مجرد التفكير أنه استخدام لأجهزة الكمبيوتر أو إدارة نظام الاتصال، إنه عصر جديد تتغير فيه أدوات التعلم والتعلم، أدوات التأثر والتأثير، أدوات تحقيق النماء الاقتصادي والديمقراطية، ولهذا فإنه عصر الإجادة في تناول التدابير الملائمة، وليس أهم من النظام القانوني بيئة وموطنا لننطلق منه في إجادة التعامل مع العصر.

وحتى تكون تدابير حماية خصوصية المعلومات فاعلة فلا بد لها من الانطلاق مما يهدد المستخدم الرقمي (المستهلك) من مخاطر استخدام وسائل تقنية المعلومات عموما والإنترنت خصوصا، وتحديدا فيما يتصل بجمع البيانات الشخصية ومقارنتها وتكوين ملفات الحالة. وإدراك أنه ليس ثمة تجارة إلكترونية دون ثقة بالشبكة وتطبيقات التقنية، فالحاجة ضرورية لاتخاذ التدابير الملائمة لإشاعة الثقة بالتجارة الإلكترونية التي تهددها مخاطر الاعتداء على الخصوصية وأمن المعلومات.

فثمة شبه إجماع على أن فعالية حماية البيانات الشخصية من مخاطر تقنية المعلومات وكفالة حق المستخدم في الخصوصية المعلوماتية - إلى جانب القواعد القانونية الدستورية والتشريعية وتنظيم القطاعات وإقرار المعايير - تتطلب وضوح الرؤية بشأن أهمية وجود وطبيعة دور الهيئات المستقلة لحماية البيانات وبقية الهيئات ذات العلاقة بتقنية المعلومات، كهيئات حرية المعلومات وهيئات التجارة الإلكترونية (سلطات التوثيق وسلطات التشفير

والتواقيع الرقمية وسلطات أمن المعلومات إن وجدت) وهو ما يوجب أن تكون هيئات حماية البيانات - من بينها - هيئات تحظى بسلطات واسعة في حقل الرقابة وتطوير القانون، مؤهلة ومدركة للمعايير القانونية المتوازنة في حقل تقييد حق الخصوصية أو إعمال استثناءاته، أو أن تتعدد مهام الهيئة لأكثر من مجرد الحماية وتحديدا عندما يكون ثمة تعارض ما أو عدم دقة في معيار التوازن بين ما توجبه هذه التشريعات وما توجبه مبادئ حماية البيانات. وفي هذا الإطار، تبين لنا أن ثمة نماذج - من اتجاه تشريعي ربما يتعاظم في القريب العاجل - للربط بين حرية الوصول للمعلومات والحق في حماية خصوصية المعلومات أو البيانات الشخصية وإيجاد معيار توازن بينهما ومحاولة توحيد جهة الإشراف أو معايير الإشراف عند تعدد الجهات.

- إلا أن هناك مبادئ للحماية في حالة القيام بمعالجة البيانات الشخصية **(الفرع الأول)**.
- تتضاعف حال معالجة البيانات الشخصية الحساسة.**(الفرع الثاني)**.

الفرع الأول

معالجة البيانات الشخصية

يمكن القول بأن معالجة البيانات الإلكترونية (بالإنجليزية: Electronic data processing) [1] تشير إلى استخدام الأساليب الآلية لمعالجة البيانات التجارية.

وعادة ما يكون هذا الاستخدام بسيطا نسبياً لمعالجة الكميات الكبيرة من المعلومات المتشابهة للأنشطة المتكررة. على سبيل المثال: تطبيق التحديثات على جرد المخزون، وتطبيق المعاملات المصرفية على الحسابات والملفات الرئيسة للعملاء، وإجراءات الحجوزات والتذاكر على نظام الحجز على خطوط الطيران، وفواتير خدمات المرافق.

أنشأ أول حاسوب للأعمال التجارية في المملكة المتحدة عام 1951 بواسطة شركة ليون جي (J. Lyons and Co.) شركة أغذية، وهو ما كان يعرف ب 'مكتب ليون الإلكتروني ' Lyons Electronic Office - أو الاختصار LEO. وقد طور أكثر واستخدم على نطاق واسع خلال الستينات وأوائل السبعينات الميلادية. (ليون جو أسس شركة منفصلة لتطوير أجهزة الكمبيوتر ل LEO ومن ثم الاندماج لاحقاً لتشكيل شركة الكهرباء الإنجليزية ليو ماركوني ومن ثم شركة الكمبيوتر الدولية المحدودة)[1] النظم التجارية المبكرة تم تركيبها حصرياً بواسطة المنظمات الكبيرة، حيث يمكنها تحمل الاستثمار للوقت ورأس المال اللازم لشراء المعدات، وتعيين موظفين متخصصين لتطوير البرمجيات المطلوبة والعمل من خلال النتائج المترتبة على ذلك (وفي كثير من الأحيان غير المتوقعة) التغييرات التنظيمية والثقافية.

---

(1) shraddha، Peter J. Lyons & Co.: LEO Computers (2002) P.25

في البداية، طورت المنظمات الفردية البرمجيات الخاصة بها، بما في ذلك مزايا إدارة البيانات بأنفسهم، ولمنتجات مختلفة ربما أيضاً حتى طلبات لبرمجيات قد تكون لمرة واحدة.

وأدى هذا النهج المجزأ إلى ازدواجية الجهود، وإلى الحاجة إلى جهود يدوية لإنتاج المعلومات الإدارية. أجبر ارتفاع تكاليف الأجهزة، والسرعات البطيئة نسبياً للمعالجة المطورين إلى استخدام الموارد بشكل فعّال. على سبيل المثال دمجت كثير من تنسيقات تخزين البيانات. والمثال الشائع هو إزالة القرن من التواريخ والذي أدى في النهاية إلى 'علة الألفية'.

إدخال البيانات يتطلب معالجة وسيطة بواسطة شريط ورقي مثقب أو بطاقة مثقبة وإدخال منفصل لمهمة عمل مكثفة ومتكررة، والتخلص من تحكم المستخدم والعرضة للخطأ.

وتحتاج البيانات غير الصحيحة أو غير الصالحة إلى تصحيح وإعادة تقديمها مع النتائج المترتبة لتسوية البيانات والحسابات. تخزين البيانات كان متسلسل بشكل صارم على الشريط الورقي، ثم لاحقاً على الشريط المغناطيسي: لم يكن استخدام تخزين البيانات في إطار ذاكرة يسهل الوصول إليها فعال من حيث التكلفة.

كما هو الحال مع غيرها من العمليات الصناعية تكنولوجيا المعلومات التجارية تحركت في جميع النواحي من المطالب، والصناعة الحرفية حيثما كان المنتج يفصل ليناسب المستهلك؛ إلى مكونات الاستخدام المتعدد لتترك الرف لتجد الأفضل ملائمة لأية حالة. مقدار الإنتاج خفض بدرجة كبيرة التكاليف وأصبحت تكنولوجيا المعلومات متاحة لأصغر شركة.

وكان LEO يصمم الأجهزة خصيصاً لعميل واحد. واليوم رقائق إنتل بنتيوم Intel Pentium والمتوافقة هي المعيار، وأصبحت أجزاء من المكونات الأخرى التي يتم تجميع حسب الحاجة. التغيير الفردي الوحيد

الملاحظ كان التحرير لأجهزة الكمبيوتر والتخزين القابلة للإزالة من البيئات المحمية والنقية الهواء.

وفي أوقات مختلفة كانت شركة مايكروسوفت Microsoft وآي بي إم IBM مؤثرة بما فيه الكفاية لفرض النظام على تكنولوجيا المعلومات، والتوحيد القياسي الناتج سمح للبرمجيات المتخصصة بالازدهار.

البرمجيات المتاحة من على الرف: وبصرف النظر عن منتجات مايكروسوفت مثل المكتب، أو لوتس، هناك أيضا مجموعات متخصصة لإدارة شؤون الموظفين والرواتب، وإدارة وصيانة حسابات العملاء على سبيل المثال لا الحصر. وهذه مكونات معقدة وبدرجة عالية من التخصص لبيئات أكبر، ولكنها تعتمد على الواجهات والاتفاقيات المشتركة. وتخزين البيانات أيضاً موحد.

وقد طورت قواعد البيانات العلائقية بواسطة مختلف الموردين إلى الأشكال والاتفاقيات الدولية المشتركة. تنسيق الملفات المشتركة يمكن التشارك فيها بواسطة الأجهزة الرئيسة الكبيرة والحاسبات الشخصية المكتبية، مما يسمح بالاتصال المباشر بالإنترنت، والإدخال والتحقق بوقت حقيقي.

وفي موازاة ذلك، فإن تطوير البرمجيات مجزأ، ولا يزال هناك الفنيون المتخصصون، ولكن استخدامهم للأساليب الموحدة يتزايد حيث تكون المخرجات قابلة للتنبؤ بها، ويمكن الوصول إليها. ومن ناحية أخرى في هذا المجال، يمكن لأي مدير مكتب التلاعب في جداول البيانات أو قواعد البيانات والحصول على نتائج مقبولة.[1]

---

(1) ELEMENTARY DATA PROCESSING،Dr. Ikhu - Omoregbe N. A.&Afolorunso، A. A.،National Open University of Nigeria،Lagos.(2012) P.148

و قـد عـرف قانـون حمايـة البيانـات الشـخصية الإنجليـزي[1] والصـادر عام 1998 معالجـة البيانـات بأنها فيـما يتعلـق بالمعلومـات والبيانـات يعنـى الحصـول أو تسـجيل أو عقـد البيانـات أو المعلومـات أو تنفيـذ عمليـة أو مجموعـة مـن العمليـات عـلى المعلومـات والبيانـات بمـا في ذلـك:

(أ) تنظيـم والتكيـف أو تعديـل المعلومات أو البيانات،

(ب) اسـترجاع المعلومات، التشـاور أو اسـتخدام المعلومات أو البيانات،

(ج) الكشـف عـن المعلومـات أو البيانـات عـن طريـق نقل أو نـشر أو خلاف ذلك وإتاحتهـا، أو(د) المحـاذاة، والجمـع، حظـر، محـو أو تدمـير المعلومـات أو البيانات.

أرسـت الاتفاقيـة الأوروبيـة بشـأن حمايـة الأفـراد فيـما يتعلـق بمعالجـة البيانـات الشـخصية[2] وكذلـك الإرشـاد الأوروبي رقـم 46 /1995 بشـأن حمايـة الأفـراد فيـما يتصل بمعالجـة البيانـات الشـخصية[3] وفيـما يتصـل بحريـة انتقـال هـذه البيانـات عـدة مبادئ فيـما يتعلـق بمعالجـة البيانـات الشـخصية، فبالنسـبة لمبدأ تجميـع ومعالجـة البيانـات الشـخصية تحدثـت المـادة الخامسـة والسادسـة والتاسـعة مـن الاتفاقية الأوروبية بشـأن حمايـة الأفـراد فيـما يتعلـق بمعالجـة البيانـات الشـخصية وقـد أوصـت بأنـه يجـب أن تكـون البيانـات الشـخصية التـي تمـر بالمعالجـة التلقائيـة:

(1) The Data Protection Act 1998 (DPA) is a United Kingdom Act of Parliament which defines UK law on the processing of data on identifiable living people

(2) Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data Strasbourg، 28.I.1981

(3) Directive 9546//EC of the European Parliament and of the Council of 24 October 1995 on the protection ofindividuals with regard to the processing of personal data and on the free movement of such data Official Journal L 281، 231995/11/ P. 0031

أ. تم الحصول عليها ومعالجتها بصورة عادلة وقانونية؛ تخزينها لأغراض محددة ومشروعة وعدم استخدامها بطريقة غير متوافقة مع تلك الأغراض؛ كافية وذات صلة وغير مفرطة فيما يتعلق بالأغراض التي يتم تخزينها؛ دقيقة، وعند الضرورة، وأبقى حتى الآن ؛ في الحفاظ على الشكل الذي يسمح بتحديد الموضوعات والبيانات لمدة لا تزيد مطلوب للغرض الذي يتم تخزين تلك البيانات.

أما في المادة التاسعة والتي تتعلق بالاستثناءات فلا يجوز استثناء من أحكام المواد 5 و6 و8 من هذه الاتفاقية إلا في حدود المادة التاسعة ويجوز عدم التقيد بأحكام المواد 5 و6 و8 من الاتفاقية عندما يكون الغرض: حماية أمن الدولة والسلامة العامة، والمصالح النقدية للدولة أو قمع جرائم جنائية ؛ حماية موضوع البيانات أو حقوق الآخرين وحرياتهم.

وبالنسبة لتقييد ممارسة الحقوق المنصوص عليها في المادة 8، وهي تخزين البيانات لأغراض محددة ومشروعة وعدم استخدامها بطريقه غير متوافقة مع تلك الأغراض التي قد يكون المنصوص عليها في القانون فيما يتعلق بملفات البيانات الشخصية الآلية المستخدمة للإحصاءات أو لأغراض البحث العلمي عند وجود أي خطر من الواضح تعديا خصوصية الموضوعات البيانات.

أما بالنسبة للإرشاد الأوروبي فقد أقر في المواد السادسة والسابعة ذات المبادئ حيث نص في مادته السادسة على أن الدول الأعضاء التي تقوم بمعالجه البيانات يجب أن تكون تلك البيانات معالجة بصورة عادلة وقانونية؛

جمعت لأغراض محددة وصريحة ومشروعة والتي لم تتم معالجتها مزيد بطريقة غير متوافقة مع تلك الأغراض. لا يتعارض ذلك مع ما يعتبر مزيدا من المعالجة للبيانات لأغراض تاريخية، إحصائية أو علمية ويشترط أن تقدم الدول الأعضاء الضمانات المناسبة وأن تكون الأغراض التي تم التجميع بغرضها كافية وذات صلة وغير مفرطة؛ و يجب اتخاذ كل الخطوات المعقولة

لضمان أن البيانات التي هي غير دقيقة أو غير كاملة، مع الاعتبار للأغراض التي تم جمعها أو التي يتم معالجتها من أجلها. و في المادة السابعة نصت على أنه يتعين على الدول الأعضاء أن تقدم البيانات الشخصية يمكن معالجتها إلا إذا: أعطت موضوع البيانات بشكل لا لبس فيه موافقته ؛ أو أن المعالجة ضرورية لأداء العقد موضوع البيانات التي هي طرف فيها أو من أجل اتخاذ الخطوات بناء على طلب البيانات الموضوع قبل الدخول في عقد؛ أو المعالجة ضرورية للامتثال لالتزام قانوني أو أن تكون المعالجة ضرورية من أجل حماية المصالح الحيوية للموضوع البيانات؛ أو أن تكون المعالجة ضرورية لأداء مهمة أجريت في المصلحة العامة أو في ممارسة السلطة الرسمية المخولة في وحدة تحكم أو في طرف ثالث لمن يتم الإفصاح عن البيانات.

ومما سبق نخلص إلى أن هناك شروطا واضحة وصارمة أرستها قوانين البيانات حيث إن المعالجة لا يجب أن تكون حرة ومن دون قيود وذلك حفاظا على خصوصية البيانات الشخصية المتداولة عبر الإنترنت والمستخدمة في ظل التطور التكنولوجي الهائل وعليه فإن معالجه البيانات الشخصية يجب أن تكون مقيده بالتالي نوعية البيانات الشخصية المخزنة، وأنه يجب أن تكون عادلة وقانونية، ويجب أن تكون محددة ولأسباب مشروعة، البيانات يجب أن تكون كافية وملائمة للأسباب المخزنة لها، ويجب أن تكون صحيحة ومجددة (Updated) المدة التي يجب أن يتم خلالها تخزين البيانات الشخصية.

الفرع الثاني

معالجة البيانات الشخصية الحساسة

البيانات الشخصية الحساسة يعني البيانات الشخصية التي تتكون من معلومات عن :

(أ) الأصل العرقي أو العنصري لصاحب البيانات.

(ب) آرائه السياسية.

(ج) معتقداته الدينية أو المعتقدات الأخرى ذات الطابع المماثل،(د) ما إذا كان عضوا في نقابة عمالية (بالمعنى المقصود في اتحاد التجارة وعلاقات العمل).

(هـ) صحته البدنية أو العقلية.

(و) حياته الجنسية.

لأن المعلومات حول هذه المسائل يمكن أن تستخدم بطريقة تمييزية، ومن المرجح أن تكون ذات طابع خاص، فإنه يحتاج إلى أن يعامل بحذر أكبر من البيانات الشخصية الأخرى. على وجه الخصوص، وهنا وفي حاله معالجة البيانات الشخصية الحساسة يجب أن تخضع لشروط أكثر صرامة من التي تخضع لها البيانات الشخصية حال المعالجة، بالإضافة إلى ضرورة انطباق الشروط العامة للمعالجة أيضا.

على سبيل المثال، المعلومات التي تصنف شخص ما لديه كسر في الساق عن البيانات الشخصية الحساسة، على الرغم من أن هذه المعلومات هي مسألة نسبية من حقيقة واضحة لأي شخص برؤية هذا الشخص مستخدما العكازات ولكن إدراج ذلك في قاعدة بيانات يعد من قبيل معالجة البيانات الشخصية الحساسة.

وكذلك فإن العديد من الأفراد يسطع اختياراتهم السياسية لجعل وولائهم السياسي العام، على سبيل المثال من خلال ارتداء شارات أو ريدات أو عن طريق وضع لاصق في مكان العمل أو السيارة أو المنزل وبالرغم من ذلك هناك شرطا لمعالجة البيانات الشخصية الحساسة التي تغطي المعلومات المعلنة من قبل الفرد المعني.[1]

فمثلا الدين أو العرق، أو كليهما، غالبا ما يمكن الاستدلال على ذلك بدرجات متفاوتة من اللباس أو الاسم. فترتبط العديد من الألقاب مع العرق أو دين معين، أو كليهما، وربما تدل على العرق والدين من الأفراد المعنيين. ومع ذلك، سيكون من السخف انطباق شروط معالجة البيانات الشخصية الحساسة على تلك الأسماء حين انطباق هذا المبدأ سيعني أن لوضع مثل هذه الأسماء على قواعد بيانات العملاء علينا أن نفي بشرط معالجة البيانات الشخصية الحساسة.

ومع ذلك، إذا كانت معالجة مثل هذه الأسماء على وجه التحديد لأنها أشارت إلى العرق أو الدين، على سبيل المثال لإرسال مواد التسويق للمنتجات والخدمات التي تستهدف الأفراد من أن العرق أو الدين، فإنها سوف تكون معالجة البيانات الشخصية الحساسة. في أي حال، يجب أن تأخذ الحيطة والحذر عند وضع افتراضات حول الأفراد وهل يمكن أن يكون جمع البيانات الشخصية غير دقيقة.

وقد حددت القوانين والتوجيهات[2] مبادئ متشابهه في معالجة البيانات

---

(1) Peter Jersey: Data Protection In Jersey And Other Offshore Jurisdictions 23 July 2008 Article by Wendy Benjamin، mondaq.com، visited 2012 Sep 14 P.161

(2) John Woulds A Practical Guide to the Data،Protection Act،December 2004، Published by The Constitution Unit School of Public Policy، UCL، 29-30 Tavistock Square،London P.31

الشخصية الحساسة[1] ووضعت أحكاما محدده لعقد ومعالجة المعلومات الشخصية الحساسة التي لا يمكن أن تتم معالجتها إلا في ظل ظروف صارمة وهذه الشروط تتلخص فيما يلي:

أولا: الحصول على الموافقة الصريحة من صاحب البيانات ويجب أن تكون هذه الموافقة صريحة وليس من الضروري أن تكون مكتوبة، ولكن يجب ألا يكون هناك لبس في صحة الموافقة.

ثانيا: أن تكون المعالجة ضرورية لأغراض ممارسة أو تنفيذ أي حق أو التزام أو ما يفرضه القانون على وحدة تحكم البيانات المرتبطة بالعمل. على سبيل المثال، غياب المعلومات المرضية المعالجة من أجل الحصول على أجازة مرضية.

واشترط الفقه أيضا أن تكون المعالجة ضرورية وفي تفسير ضرورية معالجة البيانات يجب أن تكون مندرجة تحت الأتي:

- أن تكون معالجه البيانات الشخصية الحساسة لمصلحه حيوية لصاحب البيانات أو شخص آخر في حالة عدم القدرة على الحصول على رضاء صاحب البيانات الشخصية مباشرة أو بالإنابة أو في حاله استحالة حصول مدير قاعدة البيانات على موافقة صاحب أو حجبها حجبا غير مبرر.

ومما سبق نخلص إلى أن وضع شروط صارمة من شأنها حماية البيانات الشخصية الحساسة قد يفرض حماية لمعالجة مثل هذه البيانات من الناحية القانونية ولكن من الناحية العملية فجميع البيانات الشخصية للأشخاص على شبكة الإنترنت مباحة سواء بالنسخ أو الحجب أو المعالجة وهنا يتثنى

---

(1) The data protection (processing of sensitive personal data) order 2000، Made 17th February 2000. Coming into force - - 1st March 2000، united kingdom P.62

وضع ضوابط قانونية قابلة للتنفيذ لمواكبة التسارع التكنولوجي والذي لا يلحق به المشرع في العالم وخاصة في البيئة العربية.

و كذلك فعلى المنشآت التي تقوم باستخدام تقنية المعلومات في إدارة بيانات المنشأة وعملائها، وكذلك من تقوم منشأته على الأعمال الإلكترونية (e - Business)، أن يضعوا في اعتبارهم بعض النقاط عن خصوصية البيانات ومدى تأثيرها على عمل المنشأة وسمعتها، ومنها:

ولاء العملاء يعتمد مباشرةً بالخصوصية: يعتمد الكثير من العملاء على خدمة الإنترنت للتسوق وإجراء العمليات البنكية ومراجعة المعاملات الحكومية وأمور الرعاية الصحية، وغيرها من الخدمات، ذلك طالما أنهم يثقون بأن معلوماتهم الشخصية والمالية مؤمنة ومحمية ومتعذرة الوصول إليها من قِبل الأشخاص غير المصرح لهم بذلك. ولكن عندما تتصدع هذه الثقة، فإن ولاء العميل قد يتبخر في ثوان معدودة، فبالنسبة لهم فإن تكلفة سرقة هويتهم أو التعرض لعمليات النصب هي خطورة كافية لمنعهم من إجراء أعمال مع منشآت معروف عنها أنها غير جديرة بالثقة بإعطائهم بياناتهم الشخصية. وهذه بعض الأرقام المثيرة للانتباه التي تعكس نظرة العملاء لبياناتهم الشخصية على حسب استطلاع قام به موقع TechRepublic:

- 86% من مستخدمي الإنترنت قلقين على معلوماتهم الشخصية.
- 45% من المستخدمين لا يقومون بإدخال أسماءهم الحقيقة.
- 5% فقط يستخدمون برامج إخفاء هوية الحاسب الآلي عند اتصالهم بالإنترنت.
- 94% يطالبون بمعاقبة منتهكي الخصوصية.

و على ذلك فلابد من إرساء بعض المبادئ حال معالجه البيانات وهي أن تقنية المعلومات تتحمل معظم عبء انتهاكات الخصوصية.

وهذه بعض النقاط التي يجب أخذها بعين الاعتبار عند تصميم وتطوير النظم المعلوماتية للمنشآت:

- معرفة نوع البيانات التي تتعامل معها والتي تحتوي على معلومات شخصية مُعرِّفة (Personally Identifiable Information)، مثل اسم المستخدم وكلمات المرور والعناوين البريدية وبطاقات الائتمان وأرقام الضمان الاجتماعي وغيرها. وعدم تجميع بيانات أكثر من اللازم، لأنها عبء على المنشأة في حفظها وحمايتها.
- تنفيذ آليات لتبليغ المستخدمين عند تجميع بياناتهم والهدف منها، وإعطاء أحقية الرفض لهم. تسجيل إقرار لرفض المستخدمين بتجميع بياناتهم قد يخدم المنشأة مستقبلاً.
- تحديد موقع نقاط الضعف في المنشأة: في التطبيقات أو قواعد البيانات أو الشبكات اللاسلكية أو نقط الدخول للشبكة أو أحد الواجهات الأخرى.
- تحديد خطوات وسياسات لتأمين وحماية المعلومات الشخصية من الدخول غير المصرح به أو إساءة الاستخدام، مثل ضوابط الوصول أو الدخول لها وخوارزميات التشفير والأمن المادي ومراجعة الحسابات (auditing).

تحديد سياسات تصنيف البيانات:

حالياً، يعتبر مديرو البيانات (Data Managers) هم المستضيفين/المتعهدين لبيانات منشآتهم، وبهذا فهم مطالبون بالنظر إلى هذه البيانات كأصل ذات قيمة ثمينة، بالإضافة إلى إدارتها بناء على ما تمثله للمنشأة أو من تمثله من العملاء.

ينبغي على المنشآت تحديد سياسات لاستخدام المعلومات الشخصية،

وتقوم بتصنيف نوع البيانات ومدى سريتها وأهميتها، بجانب توعية الموظفين بأهمية هذه المعلومات والسياسات المفروضة.

القيام بتحديد النظم الحساسة، يساعد على تحليل المخاطر:

الحصول على نظرة شاملة عن تصنيفات البيانات والأنظمة التي تعمل عليها، يساعد على استهداف المنشأة للأنظمة التي تمتلك أكثر البيانات حساسية للقيام بتحليلها بدقة للوصول إلى تحديد المخاطر التي قد تصيب سلامة وخصوصية هذه البيانات، وسبل الحماية منها.

المنشأة مسؤولة عن الإثبات:

هل تمت محاولة اختراق بياناتك؟ هل نجحت؟ ما البيانات المستهدفة؟ ما عدد العملاء الذين تم استهدافهم؟.

حتى في العمليات الفاشلة، قد تحتاج المنشأة للإفصاح عن الهجوم، وإثبات عدم تسرب أي بيانات خاصة (للعملاء أو الموظفين) للأشخاص الغير مصرح لهم.

والأهم هو تحديث وتجهيز وتفعيل دور أنظمة الحماية واكتشاف التطفل (intrusion detection) وتسجيل جميع عملياتها الاحترازية والدفاعية. ويأتي دورها هذا لمسؤوليتها عن حفظ هذه البيانات، ففي الولايات المتحدة الأمريكية، تُلزَم المنشأة التي تعرضت للهجوم وتسربت منها معلومات شخصية، بدفع 100 دولار عن كل سجل شخصي تم اختراقه.

رئيس الحقوق الشخصية (Chief Privacy Officer):

وهو المسؤول عن إنشاء سياسات الخصوصية لكل من العملاء أو الموظفين، وإعادة النظر والبت في القضايا ذات الصلة.

توضيح حدود المسؤولية:

تكثر في مشاريع تقنية المعلومات التعامل بالعقود الخارجية

(Outsourcing)، والتـي تحتـاج إلى عملية "مشـاركة البيانات" مـن الطرفين كليهما.

ولكـن مـن هـو المسـؤول عن عمليـات اخـتراق أو سرقة هـذه البيانات الشـخصية إذا حصلـت عنـد الطـرف المتعاقـد معـه أو مـن أحـد موظفيـه؟. "لا يمكـن منـع وقـوع الحـوادث دائمـاً"، ولكـن يمكـن الحصـول عـلى بعـض الضمانـات عنـد الاتفاق عـلى توقيع العقـود الخارجيـة، والأهـم مـن ذلـك هـو توثيقهـا مـن الطرفـين كليهـما، بالإضافـة إلى مشـاركة الخـبراء القانونيـين، إن لـزم الأمـر.[1]

أخـيراً، فنُذَكـر بمـا قالـه روجـر كلارك: "إن القلـق المتزايـد مـن النـاس حـول حفظ خصوصياتهـم يجـب أن يكـون رد فعـل لطريقـة اسـتخدام المنشـآت لتلـك المعلومـات وليـس لتقنيـة المعلومـات بذاتهـا"، فالتقنيـة سـلاح ذو حديـن والمسـتخدم هو مـن يحدد أي الحديـن يسـتخدم.

وللحفـاظ عـلى خصوصيتـك وخصوصية بياناتك هذه بعـض النصائح:

- قـم بقـراءة سياسـات الخصوصيـة (Privacy Policy) قبـل تسـجيل أي بيانـات خاصـة بـك في مواقـع الإنترنـت، وكـن حـذرا دائمـاً عنـد تسـجيل البيانـات الخصوصيـة.
- تأكـد مـن أن الموقـع يسـتخدم إحـدى تقنيـات التشـفير، ويمكـن معرفـة ذلك مـن عنـوان الموقـع (URL Address)، مثـلاً أن يبـدأ العنـوان ب https، وتأكـد مـن وجـود علامـة القفـل في زاويـة الشاشـة.
- قـم بقـراءة اتفاقيـات الاسـتخدام قبـل تنصيـب البرامـج. قـم بفحـص دوري للبرامـج التـي تعمـل في جهـازك وتسـتخدم إحـدى المنافـذ لديـك للاتصـال بشـبكة الإنترنـت وذلـك بتنفيـذ الأمر التـالي (Start - > Run - > Netstat)، أو باسـتخدام أحـد برامـج مراقبـة المنافـذ مثـل البرنامـج المجـاني Spybot Search and Distroy.

(1) Lee Bygrave Special Issue: Contemporary Issues in Internet Governance، Volume 22 Issue 1 Spring 2014 P6

- لا تقم بالاتصال بالإنترنت باستخدام شبكة لاسلكية مجهولة أو لا تستخدم أحد بروتوكولات الحماية الحديثة مثل WPA2. قم بتغيير الإعدادات الافتراضية المستخدمة من الشركة المصنعة، مثل اسم الجهاز وكلمات المرور.

- قم بتبليغ الجهات المختصة عند اكتشافك لمواقع مشبوهة، وعند تعرض جهازك لأي اختراق أمني وتسرب معلومات خاصة عنك أو عن عملائك. ويمكنك الحصول على بعض النصائح التوعوية في استخدام تقنية المعلومات عن طريق زيارة.[1]

ويرى الباحث أنه في حقل حماية البيانات الشخصية عبر الإنترنت تخلص إلى أن صاحب البيانات الشخصية هو مالكها الوحيد ومن له الحق في التصرف فيها سواء بنشرها أو حجبها ومن ثم لاختلاف ملكية البيانات عن غيرها من الممتلكات واختلاف طبيعة التعامل معها فقد أرست مبادئ عامة لحقوق أصحاب البيانات من حيث الاعتراض على معالجة البيانات الشخصية، والحصول على التعويض الملائم في حال الفشل من قبل وحده التحكم في البيانات عن حفظ تلك البيانات بالإضافة إلى تصحيح، ومنع، ومحو أو تدمير البيانات الشخصية غير الدقيقة، ولكن هذه المبادئ تحتاج إلى ظهير تشريعي ومن ثم ينبغي توفير الحماية الدستورية القوية للخصوصية، وينبغي أن يتضمن ذلك تدابير الحماية الإيجابية لهذه الحقوق ومن الأفضل فرض إلزام إيجابي على الدولة لتوفير الحماية ضد أي تدخل في هذه الحقوق.

وكذلك يجب أن ينص الدستور على قيود محدودة فقط على كل من الخصوصية وحرية التعبير، وينبغي تصميم هذا النظام بما يتكيف مع التناقضات بين هذين الحقين من خلال عملية تقييم المصلحة العامة العليا. وفي حال غياب الاعتبارات التعويضية القوية، فإن هذا سيفسر بطريقة

---

(1) Roger Clarke،Introduction to Dataveillance and Information Privacy، and Definitions of Terms Xamax Consultancy Pty Ltd،2013، P203

تفتح المجال للجدل حول مسائل الاهتمام العام، حتى ولو كان هذا يتضمن الكشف عن معلومات خاصة.

وبما أن الدستور يحتل قمة النظام القانوني وتتضمن معظم الدساتير لوائح أو مواثيق حقوق، بما يكفل حقوق الإنسان الأساسية، ولعله من المدهش أن الكثير منها لا تتضمن الحماية المباشرة للخصوصية في دساتيرها، على الرغم من قيام المحاكم بتفسير ذلك في قراراتها في الكثير من القضايا.

من الواضح أن أفضل الممارسات هي توفير الحماية للخصوصية في الدستور، وعلى الرغم من ذلك، فإن من المعقد غالباً تعديل الدساتير، وهو ما يجب أن تكون عليه، ولا يتم تعديلها إلا بعد استفتاء عام على نطاق واسع، وذلك للتأكد من أن الدستور يعكس الإرادة السائدة، ويستقطب تأييداً من الشعب واسع النطاق.

وتعد قواعد تنظيم حماية البيانات هي الأوسع نطاقاً حيث إنها تنطبق على جميع معلومات التعريف الشخصية، بينما تنطبق الخصوصية فقط على المعلومات التي من المتوقع أن يتواجد فيها قدر معقول من الخصوصية، وتعد قواعد تنظيم حماية البيانات هي الأقل شمولاً، حيث إنها تنطبق فقط على مجموعة البيانات، وعادة ما تخضع للمعالجة الآلية، وبالتالي، فإنها لا تنطبق على المعلومات الموجودة لدى وسائل الإعلام بموجب استقصاء أي فساد محتمل من جانب أي مسؤول. وتعتبر التفرقة أمر مهم جداً حيث إنه في حين تضمن معظم أنظمة حماية البيانات عدداً من القواعد المحددة لحماية المصالح العامة المختلفة.

وكذلك يجب أن تلتزم الدول ببذل جهود لرفع مستوى الوعي بشأن الخصوصية والتقنيات الجديدة، والتي تستهدف الشباب من خلال النظام المدرسي وباستخدام نظم أخرى للوصول إلى الكبار.

كما يجب على الجهات الفاعلة الأخرى التي يمكنها وضعها من رفع

مستوى الوعي - مثل الشركات وأولياء الأمور ومؤسسات المجتمع المدني - أن يؤدوا دوراً في تعزيز فهم أفضل بين الجمهور العام حول الخصوصية والتقنيات الجديدة.

بالإضافة إلى أن هناك ثمة دور حيوي لوسائل الإعلام في رفع مستوى الوعي حول أهمية الخصوصية وظهور التحديات المختلفة مع تطور شبكة الإنترنت، وتظهر الأحداث الأخيرة في المملكة المتحدة لبريطانيا العظمى وأيرلندا الشمالية. كما لا يمكن لأي مجموعة من التوصيات حول الخصوصية وحرية التعبير على شبكة الإنترنت أن تكتمل دون الإشارة إلى الجمهور العام، أي المستخدمين الرئيسيين للإنترنت. حيث يمكن فعل المزيد من قبل المستخدمين لحماية خصوصياتهم وحريتهم في التعبير على الإنترنت.

الفصل الثاني

الحماية الجنائية للبيانات الشخصية التي تتداول عبر الإنترنت

ترتبط حماية البيانات الشخصية عبر الإنترنت ارتباطا وثيقا بجرائم الكمبيوتر والإنترنت، فوفقا للتطور التكنولوجي لا يمكن دراسة ذلك النوع من الحماية دون الرجوع إلى البيئة التي تتم فيها الجريمة وبالتالي فتعتبر الجريمة الإلكترونية وعقوبتها بمثابة الظهير الجنائي لتلك الحماية.

ومن الملاحظ أن الجرائم الإلكترونية التي تتم عن طريق وسيط إلكتروني عادة ما يكون محلها بيانات شخصية فإما أن تكون المحل الأصلي للجريمة أو تستخدم لإتمام الجريمة مثل جرائم النصب.

1. وهنا يثور التساؤل حول الإطار القانوني لمواجهة الجريمة الإلكترونية **(المبحث الأول)**.
2. وما الفرق بين الجريمة الإلكترونية والجريمة المعلوماتية؟ **(المبحث الثاني)**.

المبحث الأول

الحماية الجنائية للبيانات الشخصية وجرائم الكمبيوتر والإنترنت في القوانين المقارنة

إن التتبع الأولي لنصوص التشريعات الخاصة أو نصوص القوانين المعدلة لقوانين العقوبات والخاصة بمواجهة ظاهرة جرائم الحاسوب، يظهر لنا بعض الحقائق فمثلاً:

هذه التشريعات تتفاوت في تحديد الأنماط الجرمية الجديدة والنص على تجريمها وعقابها، لكنها في مجموعها لا تخرج عن نطاق الحد الأدنى لهذه الجرائم الذي بيناه لدى استعراض جهود المنظمات الإقليمية الدولية.

والنصوص التي انطوت عليها التشريعات المقارنة بشأن جرائم الحاسوب تحدد محل الاعتداء بمعطيات الحاسوب بمدلولها التقني الواسع سواء ارتكب الفعل عليها مباشرة أم استخدم لتسهيل ارتكاب فعل آخر، وأساس التجريم الاعتداء على المعطيات لا وصف الفعل الذي سهل استخدام الحاسوب، أو الأدق، معطيات الحاسوب لارتكابه.

ونجد أن العديد من النظم القانونية المقارنة اتجهت إلى إضافة صور التجريم الجديدة إلى نصوص القسم الخاص من قوانين العقوبات في نظمها القانونية، وفي ذلك إقرار بانطباق الأحكام العامة عليها من جهة، وتفضيل لآلية ضم هذه الجرائم إلى قانون العقوبات بدلا من أفراد قوانين خاصة من جهة أخرى، ونجد هذا المسلك قد تبنته توصيات المؤتمر السادس للجمعية المصرية للقانون الجنائي.[1]

---

(1) مصطفى محمد موسى، أساليب إجرامية بالتقنية الرقمية (ماهيتها ومكافحتها)، دار الكتب القانونية،2005 ص 37.

ولكن هذا ليس الاتجاه الوحيد بل اتجهت العديد من الدول إلى إفراد قوانين خاصة تنظم مسائل جرائم الكمبيوتر والإنترنت، كما في القانون الأمريكي والقانون البريطاني وغيرها، حيث أفردت قوانين خاصة بجرائم الحاسوب، وكذلك العقوبات التي قررتها هذه القوانين، تجمع في غالبيتها بين العقوبات المانعة للحرية والعقوبات المالية لأثرهما مجتمعتين في مواجهة مخاطر وخسائر هذه الجرائم، كما أن بعض القوانين، كالفرنسي مثلا، نص على عقوبات تكميلية تتمثل بمصادرة الأجهزة المستخدمة في الجريمة وهذا مسلك حسن لأثره الشخصي (في نفسية الفاعل) والموضوعي في فعالية مواجهة هذا النوع من الجرائم.[1]

و تظهر الصياغة الفنية لنصوص التجريم في القوانين المقارنة بشأن جرائم الكمبيوتر والإنترنت، مراعاة الجوانب التقنية (التوصل بالنظام، البقاء في النظام الاختراق، المحو والتعديل، المعالجة الآلية وغير ذلك)، كما تبتعد الصياغة من حيث استخدام المصطلحات القانونية الدالة على الجرائم عن المصطلحات التقليدية - في أغلبها. والمستخدم من المصطلحات التقليدية (كالاحتيال، أو الغش، أو الإتلاف، أو الاستيلاء، أو السرقة في جريمة سرقة وقت الحاسب فقط) تتخذ مدلولات تختلف في جوانب كثيرة عن مدلولاتها التقليدية.[2]

ولقد كانت الولايات المتحدة الأمريكية بين الدول الأولى التي أحست بالحاجة إلى تشريع مستقل بشأن جرائم الكمبيوتر طبقته على الصعيدين الاتحادي أو على صعيد الولايات على حد سواء كما تتميز الولايات المتحدة الأمريكية بوجود أكبر حزمة تشريعية تغطي مسائل جرائم الكمبيوتر والإنترنت والاتصالات.

---

(1) د. سعيد عبد اللطيف علي الجرائم الناشئة عن استخدام الحاسب الآلي كلية الشريعة والقانون القاهرة، 1999 ص 163.

(2) د. عبد الفتاح حجازي – الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت – دار الكتب القانونية – 2002 ص 65.

وأمـا في أوروبـا فـإن الثمانينـات والتسـعينات شـهدت سـن قوانـين جرائـم الكمبيوتـر عـلى المسـتوى الوطنـي لـدى غالبيـة إن لم يكـن كافـة الـدول الأوروبيـة، طبعـا إلى جانـب الجهـد التشريعـي الجماعـي في إطـار أوروبـا الموحـدة، وذات الفـترة شـهدت حركـة تشريعيـة في هـذا الحقـل في أسـتراليا وكنـدا ودول مـن شرق آسـيا وأمريـكا اللاتينيـة.[1]

لقـد بـرز جليـا الجهـد التشريـع الوطنـي في النظم المقارنـة وتمثل بسـن تشريعات لمواجهـة جرائـم الكمبيوتـر الواقعـة عـلى المعطيـات ذات القيمـة الماليـة أو مـا سـميت الجرائـم الماليـة المرتبطـة بالكمبيوتـر وقـد بـدأت هـذه المرحلـة بشـكل أسـاسي وواضـح في مطلـع الثمانينـات - مـع أنهـا انطلقـت في السـبعينات بالنسـبة للولايـات المتحـدة الأمريكيـة - وذلـك مـع تطـور وسـائل الاسـتيلاء عـلى أمـوال البنـوك والاعتداء عـلى نظم الحواسـيب بالإتـلاف والتجسـس وسرقـة البيانـات.

وشـهدت الـدول المتقدمـة ولادة تشريعـات خاصـة أو تعديـل لقوانـين العقوبـات للنـص عـلى هـذه الجرائـم بعـد أن أدركـت أن النصـوص التقليديـة القائمـة لا تجـرم غـير الأفعـال الواقعـة عـلى الأمـوال الماديـة المنقولـة، هـذا بالرغـم مـن أن تشريعاتهـا تتميـز بإمـكان التفسـير الواسـع لنصوصهـا خلافـا لنصـوص قوانـين الـدول العربيـة التـي تحـصر الأفعـال الجرميـة (بوجـه عـام) بمـا يقـع عـلى الأمـوال الماديـة دون المعنويـة (طبعـا في حقـل جرائـم الأمـوال) ولا تتضمـن العبـارات التي تسـاعد على توسـيع تفسـيرها ليشـمل معطيـات الكمبيوتـر (بوصفهـا ذات طبيعـة معنويـة).

وقـد وضعـت هـذه الـدول تشريعاتهـا في هـذا الإطـار عـلى التـوالي منـذ عـام 1975 في أمريـكا، وامتـدت عـلى مـدى الثمانينـات والتسـعينات وخضعـت للتعديـل والتطويـر في ضـوء اتسـاع أنشـطة (الهاكـرز) في نهايـة الثمانينـات، ومـن ثـم شـيوع اسـتخدام شـبكة الإنترنـت ومـا أوجدتـه مـن أنمـاط جديـدة واسـتغلال

(1) Moore، R. "Cyber crime: Investigating High - Technology Computer Crime،" Cleveland، Mississippi: Anderson Publishing. (2005) P.153

لقدراتها الربطية في إنفاذ جرائم الكمبيوتر، وبالعموم فإن شبكة الإنترنت أدت إلى شيوع جرائم الدخول غير المصرح به وتجاوزت إجراءات الأمن ونشر الفيروسات وأفعال تعطيل وإنكار الخدمة وإتلاف محتوى البريد الإلكتروني أو تحويره، وأفعال إثارة الأحقاد والتعرض لحياة الأفراد وسمعتهم، وجرائم استغلال مواقع الإنترنت في الأفعال غير المشروعة والمحتوى غير المشروع كترويج المواد الإباحية والقمار[1].

- هنا يجب التساؤل عن الإطار القانوني لجرائم الكمبيوتر والإنترنت في الولايات المتحدة (**المطلب الأول**).
- وكندا (**المطلب الثاني**).
- ثم البحث في الوضع الأوروبي(**المطلب الثالث**).

---

(1) Paul Taylor. Hackers: Crime in the Digital Sublime (November 3، 1999 ed.). Routledge; 1 edition P.243

المطلب الأول

الإطار القانوني لجرائم الكمبيوتر والإنترنت في الولايات المتحدة الأمريكية

إن الولايات المتحدة الأمريكية، لا تتميز بأسبقية سن هذه التشريعات فحسب، بل تتميز بسن تشريعات خاصة بكافة مسائل تقنية المعلومات وفي قطاعات الحوسبة والاتصالات والإنترنت ترتبط أو تتعلق بجرائم الكمبيوتر والإنترنت مباشرة أو على نحو غير مباشر، كما أنها تشريعات تراعي خصائصها المميزة وتتطور تبعا لتطور قطاع التقنية ذاته، وتتميز الولايات المتحدة الأمريكية أيضا بوضع عدة تشريعات على المستوى الفيدرالي وحزمة معتبرة من التشريعات على مستوى الولايات.

فعلى المستوى الفيدرالي:

تبلور نشاط لجنة الكونجرس الخاصة بحماية استخدام الحاسوب بتقديم مشروع (قانون حماية الحاسوب سنة 1984) غير أن هذا المشروع لدى عرضه ودراسته من قبل الكونجرس ولجانه المختصة، جرى التعديل على أحكامه بشكل جوهري، وجرى إقراره بعد سلسلة من التعديلات والإضافات ولم يصدر باسمه المشار إليه، فصدر قانون (غش الحاسوب وإساءة استخدامه لعام 1984) أو كما يترجم اسمه البعض (قانون الاحتيال وإساءة استخدام الحاسوب - Computer Fraud and abuse Act.) وأضيف إلى القانون مدونة القانون الأمريكي تحت قسم الجرائم.[1]

وقد نص القانون المذكور، على تجريم مجرد الاتصال دون تصريح بنظام حاسوب، وعلى الاتصال المصرح به الذي يستخدم فيه الفاعل الحاسوب

---

(1) Jarrett، H. Marshall; Bailie، Michael W. "Prosecution of Computer Crimes". Office of Legal Education Executive Office for United States Attorneys.،2010،P 67

لأغراض غير مصرح بها كتعديل أو إتلاف أو تدمير أو إفشاء المعلومات المخزنة في الحاسب، كما نص على عقاب من يرتكب فعلا من شأنه منع الاستخدام المصرح به للحاسوب"، وخضع لاحقا لتعديلات واكبت التطورات التقنية. كما صدر أيضا في الولايات المتحدة على المستوى الفيدرالي (قانون أمن الحاسوب لسنة 1987) والذي يقضي باتخاذ الوكالات الفيدرالية خطوات ملائمة لتأمين وحماية أنظمة حواسيبها، وينظم هذا القانون مستويات الحماية والرقابة عليها والمسؤولية عن إغفالها. وتوالت بعد ذلك في التسعينات التعديلات والتشريعات الفرعية والقطاعية ذات العلاقة بأمن المعلومات. [1]

أما على مستوى الولايات:

فقد سنت جميع الولايات، قوانين خاصة أو عدلت قوانين العقوبات لديها بما يكفل النص على تجريم أنشطة جرائم الحاسوب مع تباين فيما بينها سواء من حيث صور النشاط المجرم، أو من حيث آلية التعامل مع محل الاعتداء. فقد نصت قوانين بعض الولايات. على المساواة بين معطيات الكمبيوتر والأموال المادية من حيث الحكم القانوني مما يتيح انطباق نصوص التجريم التقليدية على جرائم الحاسوب باعتبارها تستهدف المعطيات المتخذة حكم الأموال المادية بنص القانون الصريح.

من هذه الولايات مثلا، ولاية ألاسكا، التي أدخل قانونها الجديد الإتلاف المعلوماتي ويدخل ضمن الحماية حماية البيانات الشخصية أو بيانات التعريف الشخصي والدالة من قريب أو بعيد على شخصية صاحبها وذلك حال الاطلاع عليها أو الاستيلاء واستغلالها بالنشر أو بالاحتيال وذلك ضمن الأموال التي تخضع لنصوص الإضرار بالمال، وكذلك ساوى قانونها بين غش الإنسان وغش الآلة، وكذلك ولاية فرجينيا التي نص قانونها على اعتبار وقت أو خدمات الحاسوب، أو خدمات المعالجة الآلية للبيانات أو

(1) Fafinski، S. Computer Misuse: Response، regulation and the law Cullompton: Willan (2009) P95

المعلومات أو البيانات المخزنة ذات الصلة بذلك مالا، وبهذا الحكم يتحقق انطباق نصوص التجريم التقليدية فيما يتصل بالاعتداء على المال.[1]

ولكن غالبية الولايات، سنت نصوصا تشريعية صريحة في تجريم أنشطة إساءة استخدام الحاسوب، فنصت قوانين كلا من أريزونا، كاليفورنيا، كولورادو، دبلاوار، فلوريدا، جورجيا، الينوى، متشجان، ميسوري، مونتانا، نيومكسيو، رودايسلاند، تينسي، أوتاوا، سكونسيت. على تجريم إتلاف القيم المعلوماتية غير المادية، وغش الحاسوب، والاستخدام غير المصرح به للحاسوب، وسرقة وقت أو خدمات الحاسوب، وإعاقة استخدامه، والتوصل غير المصرح به لتعديل أو تغيير أو إنشاء أو استخدام البيانات المخزنة في نظام الحاسوب.[2]

في الولايات المتحدة ينظم جرائم الكمبيوتر والإنترنت مجموعة من التشريعات على المستوى الفيدرالي وكذلك على المستوى المحلي في مختلف الولايات، فعلى المستوى الفيدرالي يمثل القسم (18) من قانون الولايات المتحدة التشريع الرئيس لجرائم الكمبيوتر (المادة 1030) حيث تتضمن اعتبار الأفعال التالية من قبيل الجريمة:

1 - التوصل غير المصرح به (الدخول) إلى أحد أنظمة الكمبيوتر الحكومية وكشف المعلومات السرية، وكشف المعلومات من جهة غير مصرح بها تلقيها.

2 - الدخول غير المصرح به إلى إي كمبيوتر والتوصل إلى معلومات غير مسموح الاطلاع عليها.

---

(1) Wall، D.S. Cybercrimes: The transformation of crime in the information age، Cambridge (2007) P.251

(2) Charles Doyle،Cybercrime: An Overview of the Federal Computer Fraud and Abuse Statute and Related Federal Criminal Laws ، Congressional Research Service، 2010، P82

3 - الدخول غير المصرح به إلى أي كمبيوتر ومن ثم ارتكاب احتيال.

4 - إلحاق أضرار جراء الدخول غير المصرح به سواء للنظام أو البرامج أو للمعلومات المخزنة فيه.

5 - بث أو تهديد بارتكاب ضرر لأي كمبيوتر عبر الولايات أو للتجارة الأجنبية بغرض ابتزاز أموال أو منافع من أي شخص طبيعي أو معنوي.

أما القسم (1462) من الفصل (18) من قانون الولايات المتحدة فإنه يحظر استخدام الكمبيوتر لاستيراد مواد مخلة بالآداب إلى داخل الولايات المتحدة الأمريكية.

في حين أن القسم (1463) من الفصل (18) يحظر نقل أية مواد فاحشة عبر الولايات أو الجهات خارجية.

ويجرم القسم (2251) من الفصل ذاته توظيف أي قاصر أو إغرائه في المشاركة في أنشطة جنسية بما فيها خلق وتصوير مواد وبثها لجهات خارجية.

ويحظر القسم (22051) من ذات الفصل استخدام الكمبيوتر الإخلال برعاية قاصر بقبول استغلاله - مع العلم - في إنتاج مواد تنطوي على استغلال جنسي.

ويعتبر القسمين (2252، 2252 /أ) من الفصل ذاته نقل وتبادل المواد الفاحشة ذات الصلة بالأطفال جريمة.

أما القسم (1028) من الفصل (18) من قانون الولايات المتحدة فإنه يعتبر إنتاج أو نقل أو إدارة جهاز يتضمن نظام كمبيوتر بقصد استخدامه بتزوير الوثائق أو إنتاج وثائق تعريف مزورة جريمة ويعتر القسم (2319) من الفصل ذاته الإخلال بحق المؤلف جريمة فيدرالية.

وعلى مستوى الولايات، فإن الإطار العام لتشريعات الولايات المتحدة في حقل جرائم الكمبيوتر والإنترنت يتمثل بما يلي:

1. كل ولاية من الولايات الخمسين تملك حرية التشريع الخاص بها، وليس هناك آلية على مستوى الولايات أو المستوى الفيدرالي تتطلب تبني الولاية شكلا أو محتوى محددا لقوانينها، وذلك بالرغم من وجود مشاريع توحيدية ومحاولات وتصريحات تهدف إلى توحيد التدابير التشريعية. [1]

2. إن الإطار العام لتوحيد قوانين جرائم الكمبيوتر يعتمد على مشروع قانون نموذجي تم وضعه من قبل هيئة أكاديمية عام (1998)، حيث يقسم أحكام جرائم الكمبيوتر والإنترنت إلى ثمان طوائف (ويجب أن يلاحظ أن هذا هو تقسيم القانون النموذجي لكنه يعتمد هنا كإطار للوقوف على مواقف التشريعات القائمة والنافذة في الولايات)[2]:

أ. المسائل الإجرائية.

ب. الجرائم غير المتصلة بالجنس الواقعة على الأشخاص:

عدد قليل من الولايات تعاملت مع الجرائم التي تستهدف الأشخاص

(1) H. Marshall Jarrett، Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations، Office of Legal Education Executive Office for United States Attorneys 2010، P 125

(2) Susan W. Brenner، State Cybercrime Legislation in the United States of America: A Survey، 7 RICH. J.L. & TECH. 28 (Winter 2001)، at http://www.richmond.edu/jolt/v7i3/article2.html. P.27 American Bar Association Task Force on the Federalization of Criminal Law، Report: Report on the Federalization of Criminal Law، 1998 A.B.A. SEC. CRIM. JUST. REP. 2، http://www.abanet.org/crimjust/fedreport.html. P.34

مـن غـير الجرائـم المتعلقـة بالمحتـوى الجنـسي، فـلا يوجـد أية ولايـة نصت علـى جريمـة كمبيوتـر تتعلـق بقتل الأشـخاص.

إذ ينظـر إلى اسـتخدام الكمبيوتـر بشـكل مـا أو أية واسـطة تقنية لارتـكاب جريمة القتـل، عـلى أن ذلـك مجـرد وسـيلة لإحـداث القتـل الواقـع عـلى الأشـخاص، وباعتبـار أن جرائـم القتـل تحديـدا يجـري العقـاب فيهـا عـلى النتيجـة بغـض النظـر عـن الوسـيلة المرتكبـة فيهـا، إلا إذا كانـت هـذه الوسـيلة ذات أثـر عـلى العقوبـة. أمـا ولايـة (فرجينيا) فقـد اعتـبرت اسـتخدام الكمبيوتـر أو شـبكة الكمبيوتـر بـدون تصريح بنيـة إلحاق الضرر المـادي بالأفـراد جريمـة مـن بـين جرائـم الكمبيوتر[1].

وقـد اعتـبرت (16) ولايـة مـن بـين الولايـات الأمريكيـة [2] أن إطـلاق التهديـدات والمـواد التـي تثـير الأحقـاد مـن قبيـل الأفعـال الجرميـة ومعظمهـا تتطلـب أن يكـون الجـاني قـد نقـل تهديـدا ممكـن تطبيقـه وممكـن تصديقـه Credible threat لإلحـاق إصابـة بشـخص أو ضرر بـه أو بعائلتـه أو بـأي شـخص آخـر.

وبعضهـا [3] اعتـبر مـن بـين الجرائـم السـلوك أو المسـاهمة في ارتـكاب سـلوك قـد يـؤدي بالشـخص العـاديreasonable Person A للمعانـاة مـن التهديـد أو التعـرض لإزعـاج حقيقـي أو أي ضرر آخـر، وكذلـك الخـوف مـن الإصابـة أو المـوت عـلى نفسـه أو أحـد أفـراد عائلته.

وبعضهـا جـرم الاتصـالات التـي تتضمـن مـواد بذيئـة بأيـة واسـطة إلكترونيـة تسـتهدف تهديـد شـخص أو إلحـاق الـضرر بـه أو بعائلتـه ويشـمل ذلـك اسـتخدام لغـة فاحشـة.

وفي هـذا العـام اعتـبرت محكمـة نيويـورك أن هـذا النـص ينطبـق عـلى رسـائل التهديـد والـذم التـي ترسـل عـبر الإنترنـت. وقـد تـم تقديـم مشـاريع قوانـين تجـرم

---

(1) المادة: § 18.2 - 152.7 من قانون ولاية فرجينيا VA. CODE ANN

(2) . ALA CODE § 13A - 11 - 8); ALASKA STAT.

(3) ALA. CODE § 13A - 11 - 8; ARIZ. REV. STAT

الإزعـاج والتهديـد والمضايقـة والتحـرش وتوزيـع المـواد البذيئـة أو المزعجـة في عـدد مـن الولايـات التـي لا تتضمـن قوانينهـا نصوصـا عـلى مثـل هـذه الجرائـم.

ج. الجرائـم التي تتصـل بالمواد الإباحية:

بالإضافـة إلى الجرائـم المشـار إليهـا في الطوائـف الأخـرى، فـإن معظـم الولايـات تضمنـت قوانينهـا مـواد تتعلـق بالأفعـال التـي تسـتهدف اسـتغلال أو إغـواء القـصر أو تتعلـق بدعـارة الأطفـال (Pornograptly). فبعـض الولايـات جـرم اسـتخدام الكمبيوتـر لإغـراء وإغـواء القـصر للتورط أو المشـاركة في أنشـطة جنسـية محظورة، وجرمـت العديد مـن الولايـات اسـتخدام الكمبيوتـر لجمـع المعلومـات حـول الأطفـال ومقارنتهـا بغـرض تسـهيل أو تشـجيع أو عـرض أو الحـض عـلى أنشـطة جنسـية محظـورة تتصـل بذلـك الطفـل وهـو جهـد ضمـن إطـار مكافحـة الجرائـم اللاأخلاقيـة المتصلـة بالأطفـال.

كـما أن العديـد مـن الولايـات حظـرت اسـتخدام الكمبيوتـر لإنتـاج أو تخزيـن أو توزيـع المـواد الإباحيـة المتصلـة بالأطفـال. ومعظمهـا حظـر اسـتخدام الكمبيوتـر لإرسـال المـواد الفاحشـة للأطفـال. وقـد اعتبرت ولايـة ببنسـلفانيا اسـتخدام الكمبيوتـر جريمة إذا مـا اسـتخدم للاتصـال بطفـل بغـرض إقحامـه بأنشـطة الدعارة.[1]

د. جرائـم الاختراق والتدمير:

ويعتـبر هـذا الجـزء هـو الجـزء ذو الصلـة بمحـل الدراسـة حيـث عـاده مـا يكـون الاخـتراق والتدمـير للبيانـات الشـخصية سـواء تلـك المتعلقـة بالأفـراد أو الكيانـات وبالتـالي فـإن معظـم إن لم يكـن كافـة الولايـات الأمريكيـة اهتمـت بشـكل أسـاسي بجرائـم الكمبيوتـر والإنترنـت المتصلـة بالاخـتراق وإلحـاق

---

(1) Halder، D.، & Jaishankar، KCyber crime and the Victimization of Women: Laws، Rights، and Regulations. Hershey، PA، USA: IGI Global.. (2011)، p201

الـضرر بالنظـم والشـبكات والمعطيـات جراء هذه الأنشـطة، وتنقسـم التدابـير التشريعية المتصلـة بالاخـتراق إلى طائفتين:

- طائفة تشريعـات انتهاك الحرمةTrespass.
- وطائفـة تشريعات أنشـطة التخريب Vandalism.

وهـذا التمييـز يرجـع إلى التمييـز بـين طائفتـي الهاكـرزHackers التـي تقـوم بأنشـطة الاخـتراق وانتهـاك الحرمـة دون تصريـح Hacking، وطائفـة الكريكـرز Crackers التـي تقـوم بهجـمات التدمـير انطلاقا مـن دوافع الحقـد Cracking. ومعظم الولايـات تتوفـر لديهـا تشريعـات تعتـبر الدخـول إلى نظـم الكمبيوتـر أو الشـبكات بدون ترخيـص جريمـة، وهـي مـا تعـرف بتشريعـات ال Hacking [1]، وكذلـك فـإن معظـم الولايـات وضعـت تشريعـات تحظـر هجـمات التدمـير وتعتبرها أكـثر خطورة من أنشـطة الدخـول غـير المـصرح بـه، فتقـرر عقوبـات مغلظـة عـلى الدخـول غـير المصرح بـه بقصد إلحـاق الـضرر أو تعطيـل عمـل النظـام أو الأضرار بأيـة صـورة بالنظـام أو المعطيـات، وبعضهـا يضيـف جريمـة إسـاءة اسـتخدام معلومـات الكمبيوتـر والتـي يحظـر في نطاقهـا النسـخ أو تلقـي أو اسـتخدام المعلومـات التـي تـم الحصول عليهـا كنتيجـة لإحدى جرائم الاخـتراق أو الهجـمات التدميريـة. وتعتـبر ولايـة نيويـورك مجـرد اخـتراق الكمبيوتـر بنية ارتـكاب أو محاولـة ارتـكاب أي جريمـة بمثابـة جريمـة معاقـب عليهـا. [2]

وبعـض الولايـات جـرم إنتـاج أو نقـل الفيروسـات والبرامـج الضـارة وتـم تقديـم مشـاريع قوانـين للغـرض ذاتـه في ولايـات أخـرى، وبعضهـا جعـل جريمـة

---

(1) Williams، M. "Virtually Criminal: Crime، Deviance and Regulation Online" Routledge، London (2006) P.164

(2) Jaishankar، K. (Ed.) Cyber Criminology: Exploring Internet Crimes and Criminal behavior. Boca Raton،: CRC Press، Taylor and Francis Group. (2011P 69

إدخال معلومات زائفة إلى نظام كمبيوتر من أجل تدمير أو المساس زيادة أو نقصاً بائتمان أي شخص.

وعدد من الولايات جرم الاعتداء على أجهزة الكمبيوتر أو خدمات تزويد الكمبيوتر التي تنطوي على تعديل أو إتلاف للأجهزة أو الخدمات المزودة للكمبيوترات أو نظم الكمبيوتر أو شبكات الكمبيوتر.

وأكثر من ذلك اعتبرت بعض الولايات من بين جرائم الكمبيوتر إنكار أو قطع أو إعاقة خدمة الكمبيوتر أو التسبب في تعطيل هذه الخدمة أو منع الدخول للنظام، وبعضها اعتبر تدمير معدات الكمبيوتر جريمة من بين جرائم الكمبيوتر(وهو ما يخرج عن مفهوم جرائم الكمبيوتر على نحو ما سبق إيضاحه)، واعتبرت ولاية شمال كارولينا أن التهديد بتدمير الكمبيوتر أو النظام - بقصد الحصول على مال أو أي منفعة للشخص أو لشخص آخر أو التسهيل له ارتكاب أي فعل - ارتكابا لجريمة كمبيوتر.

وقد أقامت بعض الولايات المسؤولية جراء الاعتداء على خصوصية الكمبيوتر أو المعلومات، أو عند استخدام الكمبيوتر والشبكات بقصد الرقابة أو جمع المعلومات عن الموظفين أو السجلات الطبية أو الرواتب أو القروض أو أي معلومات مالية شخصية مع توفر العلم بأن هذا النشاط غير مصرح به، في حين اعتبرت بعض الولايات إفشاء كلمة السر العائدة لشخص آخر جريمة كمبيوتر معولة أنها تعتبر من البيانات الشخصية للأفراد. [1]

هـ - جرائم احتيال الكمبيوتر وسرقة المعطيات:

جرمت غالبية الولايات المتحدة الأمريكية استخدام الكمبيوتر لارتكاب الاحتيال، كاستخدام الكمبيوتر أو الشبكة أو أي جزء منهما بقصد الحصول على المال أو المنافع أو الخدمات باستخدام وسائل وهمية أو زائفة

(1) McQuade، S. “Understanding and Managing Cybercrime”، Boston: Allyn & Bacon (2006) P.165

أو عن طريق وعود أو مظاهر كاذبة، ويلحظ توجه البعض لإدماج احتيال الكمبيوتر ضمن نصوص الاحتيال التقليدية المقررة في قوانين هذه الولايات بدل وضع نصوص تشريعية مستقلة بشأن احتيال الكمبيوتر.[1]

وأقامت عدد من الولايات المسؤولية عن سرقة الكمبيوتر والتي يمكن أن تتضمن العديد من الأفعال مثل سرقة المعلومات، وسرقة البرامج، وسرقة أجهزة الكمبيوتر، وسرقة خدمات الكمبيوتر. وجرمت غالبية الولايات استخدام الكمبيوتر لارتكاب سرقة بالمعنى التقليدي، كسرقة الممتلكات والاستيلاء على الأموال من غير المعطيات أو الأجهزة أو البرامج، وقليل من الولايات جرمت حيازة معطيات أو برامج الكمبيوتر المتحصلة من الجريمة.[2]

وقد نصت عدد من تشريعات الولايات على سرقة الهوية أو وسائط التعريف، فاعتبرت من قبيل الجريمة - متى ما توفر العلم وقصد تحقيق منافع مادية - الحصول على أو حيازة أو نقل أو استخدام، أو محاولة الحصول أو الحيازة أو النقل أو الاستخدام، لواحدة أو أكثر من وثائق التعريف الشخصية أو الأرقام الشخصية أو أية وسائل تعريفية للشخص أو لشخص آخر غير مصرح له قانونا بحيازتها، وهذه التشريعات لا توصف عموما كجزء من تشريعات جرائم الكمبيوتر، ومع ذلك يتم إدخالها ضمن نطاق تشريعات جرائم الكمبيوتر بسبب اتصال سرقة الهوية بأنشطة الاختراق والدور الرئيس الذي تلعبه هذه الأنشطة في هذا الحقل.

(1) Johanna Granville،"Dot.Con: The Dangers of Cyber Crime and a Call for Proactive Solutions،" Australian Journal of Politics and History، vol. 49، no. 1 2003)، pp. 102 - 109.

(2) Wall، D.S. Cybercrimes: The transformation of crime in the information age، Cambridge: Polity(2007) P196

و. جرائم تزوير الكمبيوتر (الوثائق والمعطيات الإلكترونية):

جرمت بعض الولايات أنشطة تزوير الكمبيوتر، ويعرف تزوير الكمبيوتر بأنه " قيام الشخص بإنشاء أو تعديل أو إلغاء أي معطيات خاصة بأي كمبيوتر أو شبكة كمبيوتر بحيث ينجم عن فعله تغيرا في الحقيقة المتعلقة بوثيقة معنوية أو تعليمات" (1). وعلى الأقل فإن ولاية واحدة اعتبرت من قبيل جرائم الكمبيوتر حيازة أجهزة ووسائل التزوير التي تشمل الكمبيوترات أو معداتها أو برامجها المصممة خصيصا أو المستخدمة في ارتكاب التزوير.

ز. المقامرة والأفعال الأخرى التي تستهدف الأخلاق والآداب العامة:

إن ولاية أمريكية واحدة فقط جرمت المقامرة على الخط وهي ولاية Louisiana، فقط اعتبرت هذه الولاية المقامرة بواسطة الكمبيوتر جريمة، ويتضمن ذلك القيام بأي سلوك أو المشاركة بسلوك يتضمن اللعب كاللوتري أو المضاربات بأنواعها تحت خطر خسارة ذلك الشخص أية قيمة، وذلك باستخدام الإنترنت أو الويب عن طريق أي كمبيوتر، كما اعتبر قانون هذه الولاية من قبيل الجريمة تطوير أو تزويد خدمات كمبيوتر أو برامج أو أي منتج آخر لدخول الإنترنت وعرض أي نشاط يتصل بالمقامرة أو بالأعمال المكونة لهذا الفعل مع توفر احتمال تحقق الخسارة وذلك بقصد تحقيق مكاسب من وراء هذا السلوك.

ويجري العمل على اتخاذ تدابير تشريعية لتجريم المقامرة على الخط في عدد من الولايات الأخرى، وعلى الأقل فإن ولاية واحدة تبنت تشريعات لتنظيم التعامل مع الكحول وبيعها عبر الإنترنت، وتتجه ولايات أخرى لوضع مثل هذا التشريع، وبعض الولايات أعد تشريعات تهدف إلى اعتبار بيع السجائر عبر الإنترنت لمواطني هذه الولايات عملا غير قانوني.(2)

---

(1) David Levi،Computer fraud charges in New York..، PC، Forest Hills، NY (May 2011) P.85

(2) Report Responding to gambling related crimes،report to Government department of tresuary and finance USA October 2011

ح. الجرائـم ضد الحكومة:

عـدد قليـل مـن الولايـات الأمريكيـة اعتـبر مـن قبيـل جرائـم الكمبيوتر اسـتخدام الكمبيوتـر لتعطيـل تطبيـق القانـون أو تعطيـل خدمـات حكوميـة، فقـط حظـرت ولايـة إلينـوي اسـتخدام الكمبيوتـر للتسـبب بتعطيـل أو قطـع أي خدمـة أو أيـة عمليـة أو إجـراءات حكوميـة محليـة أو أنشـطة المؤسسـات العامـة. والعديـد من الولايـات جرمت اسـتخدام الكمبيوتـر لتعطيـل أو قطـع أي خدمـة أساسـية، ويشـمل ذلـك خدمـات المؤسسـات العامـة والخاصـة ذات النفـع العـام والخدمـات الطبيـة وخدمـات الاتصـال وكافـة الخدمـات الحكوميـة، ويشـمل أيضـا تعريـض الأمـن العـام الخطـر.

واعتـبرت بعـض الولايـات اسـتخدام الكمبيوتـر للحصـول عـلى معلومـات تعتبرهـا الدولـة أو أيـة دائـرة سياسـية مـن قبيـل المعلومـات السرية[1].

ويحظـر قانـون ولايـة فرجينيـا الغربيـة الدخول غير المـصرح به إلى أيـة معلومات مخزنـة داخـل كمبيوتـر مملـوك أو متصـل بجهـات التشريـع بالولايـة وجـرم قانـون جزيـرة Rhode اسـتخدام الكمبيوتـر لتدمـير أي دليـل بقصـد تعطيـل أي تحقيق رسـمي، واعتـبرت ولايـة Utah عـدم الإبـلاغ عـن جريمـة الكمبيوتـر بمثابـة جريمـة.[2]

إن هنـاك ثمـة جهـود تشريعيـة واسـعة في حقـل حمايـة المعلومـات والخصوصيـة معروضـة عـلى المؤسسـات التشريعيـة في معظـم الولايـات المتحـدة الأمريكيـة، ففـي ولايــة أريزونــا هنــاك مــشروع قانــون لحظــر توفـير البيانــات الشــخصية الخاصــة

---

(1) Brenner، S. "Law in an Era of Smart Technology"، Oxford: Oxford University Press (2007) P.16

(2) J aishankar، K. Cyber Criminology: Exploring Internet Crimes and Criminal behavior. Boca Raton، FL، USA: CRC Press، Taylor and Francis Group. (Ed.) (2011). P136

بـأي موظـف حكومـي عـلى شـبكة الإنترنـت أو أي موقـع معلومـاتي أو حيـازة أي معلومـات شـخصية تهـدد بالخطـر سـلامة أي موظـف حكومـي أو سـلامة عائلتـه أو حصـول تهديـد يظهـر أنـه كان نتيجـة توفـير المعلومـات الشـخصية، وهنالـك مـشروع قانـون في ولايـة كاليفورنيـا بشـأن حظـر إفشـاء معلومـات حـول عناويـن منـازل الضبـاط والموظفـين الحكوميـين عـبر الإنترنـت.[1]

كـما أن العديـد مـن الولايـات يجـرى فيهـا نظـر مشـاريع قوانـين تتعلـق بتجريـم إرسـال البريـد الإلكـتروني غـير المرغـوب بـه أو غـير المطلـوب **spamming** وهنـاك مشروع قانـون في ولايـة نيوجـرسي يهـدف إلى تغليـظ العقوبـات عـلى جرائـم الدخـول إلى أو تدمـير أنظمـة الكمبيوتـر المنزليـة.

ويـري الباحـث أنـه بهـذه الاتجاهـات المسـتقبلية تحـرص الولايـات المتحـدة وأجهزتهـا التشريعيـة عـلى زيـادة الحمايـة للبيانـات الشـخصية المتداولـة عـبر الإنترنـت وعـلى أجهـزة الكمبيوتـر وذلـك نظـرا لتنامي الخطـر بتنامـي التطـور التكنولوجي وزيادة مخاطـر الاسـتيلاء أو اسـتغلال البيانـات الشـخصية أو بيانـات التعريـف الشـخصي.

وكذلـك فـإن مراجعـة تشريعـات جرائـم الكمبيوتـر النافـذة في مختلـف الولايـات المتحـدة الأمريكيـة يشـير إلى أهميـة التوجـه نحـو وضـع تشريـع شـامل وموحـد لمعالجة هـذه الجرائـم، بسـبب وجـود اختـلاف حقيقـي في مسـتويات الحمايـة وتحديـد أنماط هـذه الجرائـم، بـل وبسـبب الاختـلاف في الاصطلاحـات المسـتخدمة وأثر ذلك عـلى توفير الحمايـة، إضافـة إلى التبايـن بشـأن العقوبـات المقـررة لهـذه الجرائـم.

ويرجـع التبايـن والاختـلاف بـين تشريعـات الولايـات المتحـدة الأمريكيـة في هـذا الحقـل إلي عوامـل عديـدة:

---

(1) Wall، D.S.) Cybercrimes: The transformation of crime in the information age، Cambridge: Polity. 2013) : P 96

أولها: التطور السريع الذي شهدته ظاهرة جرائم الكمبيوتر والإنترنت برغم حداثة الظاهرة، وهو ما أدى إلى تباين درجة الاستجابة من ولاية إلى أخرى، خاصة في ظل عدم الاتفاق على أنماط الجرائم ومحدداتها، بل وعلى مفاهيم الاصطلاحات المتصلة بها والعناصر المتضمنة فيها، وأكثر من ذلك الخلط والتشتت الحاصل بشأن الكثير من المفاهيم المتصلة بهذه الظاهرة.

وأما العامل الثاني: فهو عامل قديم جديد، يتمثل باستمرار حالة الخلاف بشأن ما إذا كانت جرائم الكمبيوتر والإنترنت ظاهرة جديدة تتطلب تشريعات خاصة أو أنها مجرد وسائل جديدة لارتكاب جرائم تقليدية لا تحتاج إلى نصوص جديدة، وأكثر ما تحتاجه مجرد إعادة مراجعة النصوص القائمة، هذا على الرغم من أن الاتجاه الفقهي العام في مختلف دول العالم قد حسم لصالح وجوب التعامل مع جرائم الكمبيوتر كظاهرة جديدة تتطلب تدابير تشريعية خاصة.

أما العامل الثالث: فهو الطبيعة المعقدة لجرائم الكمبيوتر والسمة المميزة لها باعتبارها جرائم عابرة للحدود تتطلب تعاونا وتنسيقا فيما بين الدول وتجعل التدابير المحلية غير ذات أثر ما لم يتحقق انسجاما دوليا في أنشطة المكافحة، ومن هنا فإن كل ولاية تنظر لمفهوم تحقيق نصوصها لمتطلبات التعاون الدولي وفق مفهومها الخاص.

إن الحقيقة التي تظهر جراء مراجعة مختلف تشريعات جرائم الكمبيوتر والإنترنت في الولايات المتحدة هي أن هناك فجوة بين بناء وفعالية هذه التشريعات مقارنة بتشريعات الجرائم التقليدية أو ما يسمى بجرائم العالم الحقيقي، ولعل مرد ذلك للطبيعة الخاصة لجرائم الكمبيوتر والآثار المختلفة لها عن غيرها من الجرائم، واتصال الأفعال فيها بإحداث مساس بالكافة بل وبالعناصر الأساسية في بناء المجتمع ونظامه السياسي والاقتصادي

والاجتماعي، وستظل تشريعات جرائم الكمبيوتر في أية دولة غير ذات أثر في ظل إغفال الحاجة الملحة للتحرك الدولي الشامل لمكافحة خطر هذه الجرائم وحل مشكلات الاختصاص وتنازع القوانين ومشكلات صلاحيات جهات التحقيق الوطنية خارج الحدود وتنظيم أنشطة الملاحقة ضمن تعاون دولي متوازن وفاعل.

المطلب الثاني

الإطار القانوني لجرائم الكمبيوتر والإنترنت في كندا

قبل الانتقال للتجربة الأوروبية من المفيد الإشارة بإيجاز للتجربة الكندية باعتبارها الدولة الثانية التي تشكل القارة الأمريكية الشمالية، حيث عدل المشرع قانون العقوبات في عام 1985، فعاقب استنادا إلى التعديل كل من أوقف أو اعترض بطريق الغش أو بدون وجه حق أو تسبب في إعاقة أو عرقلة أي من وظائف الكمبيوتر، كما عاقب على الحصول بغش على خدمات الكمبيوتر، وعلى استخدام أو التسبب في استخدام الكمبيوتر لارتكاب أي من الأفعال المذكورة (م2/301)، وعاقب في المادة ذاتها على إتلاف البيانات وحدد الأفعال المنطوية تحت هذا الوصف.

وعدل القانون تعريف الوثيقة التقليدي المعتبر في جريمة التزوير لتشمل أية مادة يتم التسجيل عليها من قبل إنسان أو كمبيوتر لغايات تتجاوز مشكلة مفهوم المحرر المادي وتطلبه كمحل لجرم التزوير.[1]

---

(1) Avner Levin،International Comparison of Cyber Crime، PRIVACY AND CYBER CRIME INSTITUTE،2013 P 51. See also Stein Schjolberg، CybercrimeData AS. Cybercrime laws from around the world. Norway. (2013). Available http://www.cybercrimelaw.net/Cybercrimelaws.html. .

المطلب الثالث

الإطار القانوني لجرائم الكمبيوتر في أوروبا

تقدم الاتفاقية الأوروبية لجرائم الكمبيوتر ولأول مرة إطارا لتحديد قائمة جرائم الكمبيوتر وأنماطها وطوائفها، إذ حتى الآن وبالرغم من الجهود التشريعية والتدابير الإقليمية والدولية على مدى السنوات الثلاثين الماضية لم تتوفر رؤية شاملة أو إطار واضح يحدد قائمة الجرائم أو بين أساس التقسيم، ولهذا فإن أهم ما يسجل لهذه الاتفاقية أنها تطرح إطارا للتقسيم والتحديد بشأن القواعد الموضوعية لجرائم الكمبيوتر والإنترنت.[1]

وبالرجوع إلى المعيار الذي اعتمدته، نجده بالأساس يقوم على فكرة دور الكمبيوتر بالجريمة.

فالطائفة الأولى التي نصت عليها الاتفاقية، والتي أطلقت عليها الجرائم التي تستهدف سرية وسلامة وتوفر المعلومات، هي في الحقيقة الجرائم التي يلعب الكمبيوتر فيها دور الهدف، أي الجرائم التي تستهدف معطيات الكمبيوتر والبيانات المسجلة عليه بذاتها سواء لجهة الوصول إليها أو الاطلاع عليها أو إفشائها أو تحويرها أو إتلافها، وهي المعطيات في مراحل المعالجة والتخزين والنقل بواسطة أجهزة الكمبيوتر ووسائل الاتصال وشبكات المعلومات.

ونجد الطائفة الثانية: وهي ما أطلقت عليها الاتفاقية الجرائم المرتبطة بالكمبيوتر وهي الجرائم التي يلعب الكمبيوتر فيها دور

---

(1) الإتفاقيه الأوروبية حول برامج الكمبيوتر:

available at http://isper.escwa.un.org/FocusAreas/CyberLegislation/Index6/tabid/198/language/en - US/Default.aspx

الوسـيلة، أي الأداة المسـتخدمة لارتـكاب جـرم تقليـدي كالاحتيـال والتزويـر.

وأما الطائفة الثالثة: والتي أطلق عليها تعتبر الجرائم المرتبطة بالمحتوى، فهي الجرائم التي يلعب فيها الكمبيوتر دور البيئة الجرمية، وقد حصرتها الاتفاقية بجرائم المواد اللاأخلاقية المتصلة بالأطفال أو المتعلقة بهم، ولا تنص الاتفاقية على بقية أنماط جرائم المحتوى كالمقامرة والجرائم المرتبطة بالمخدرات أو غيرها.

أما الطائفة الرابعة: المتعلقة بجرائم الملكية الفكرية، فهو نص مكمل لقواعد لحماية الجزائية في هذا الحقل المقرر وطنيا ودولياً.[1]

ويلاحظ في معرض الحديث عن قائمة الجرائم أن الاتفاقية جعلت الاستيلاء على البيانات في إطار مفهوم الجرائم التي تستهدف السرية وسلامة وتوفر المعلومات، وفي النطاق ذاته يمكن إدخال الأنماط المختلفة لجرائم البريد الإلكتروني والتراسل الإلكتروني، ولقد ابتعدت عن الوصف الفرعي أو التفصيلي لأنماط السلوك الإجرامي أو الصور التي تتخذها الجريمة الواحدة أو التي تندرج في نطاق الجريمة الواحدة، وهذا مسلك محمود باعتبار أن توصيف السلوك في الغالب يتصل بالوسائل الإلكترونية المتبعة في ارتكاب الجريمة.[2]

أما ما يتعلق بجرائم الخصوصية أو بشكل أدق الجرائم التي تستهدف البيانات الشخصية في مراحل الجمع والمعالجة والاستخدام والنقل، فإن الإطار العام للنصوص الموضوعية لم يميز نوعية المعطيات، وأما إذا كانت

---

(1) Council of Europe، Project on Cybercrime. (032007/13/). Cybercrime legislation – country profile. United States of America. URL: http://www.cyberlawdb.com/docs/usa/usa.pdf. retrived 012013/17/

(2) McCullagh، Declan; Anne Broache ("Senate Ratifies Controversial Cybercrime Treaty، UIJ press t 2006 P 46.

بيانـات تتصـل بالشـخص أو بمصالـح اقتصاديـة أو ماليـة أو مسـائل أمنيـة أو غـير ذلـك، ولعـل مـرد هـذا الاتجـاه السـعي لتعميـم حمايـة المعطيـات بكافـة أنواعهـا إضافـة إلى أن مسـائل حمايـة البيانـات الشـخصية والخصوصيـة – كـما أسـلفنا - تحظـى بتنظيـم تشريعـي قائـم بـل وأكـثر تميـزا عـن التنظيـم التشريعـي لجرائـم الكمبيوتـر، إذ يغطـي هـذا الموضـوع بالاتفاقيـة الأوروبيـة لحمايـة البيانـات الشـخصية وبقائمـة طويلـة مـن التشريعـات الوطنيـة والأدلـة الإرشـادية في نطـاق أوروبـا الموحـدة.[1]

بقـي أن نشـير إلى أن جرائـم التجسـس الصناعـي وجرائـم الأسرار التجاريـة المرتبطـة بالكمبيوتـر لم يجـر النـص عليهـا صراحـة، وهـو مـا يرجـع إلى أن بقيـة النصـوص وتحديـدا الطائفـة الأولى المتعلقـة بالجرائـم التـي تسـتهدف سريـة وسـلامة وتوفـر المعلومـات، تغطـي أنشـطة التجسـس باعتبارهـا دخـولا غـير مصرح بـه إلى النظـم وكشـف للمعلومـات المخزنـة فيهـا وإفشـاء لهـا.

وأمـا عـن نصـوص المسـائل الإجرائيـة فإنهـا تتخـذ أهميـة قصـوى، ذلـك أن التدابـير التشريعيـة الإجرائيـة لم تكـن بمسـتوى التدابـير التشريعيـة الموضوعيـة، وهـي غائبـة لـلآن في الجـزء الأكـبر مـن دول الاتحـاد الأوروبي، طبعـا فيـما يتعلـق بالقواعـد الإجرائيـة الخاصـة بجرائـم الكمبيوتـر والإنترنـت، وتمثـل أحـكام الاتفاقيـة في هـذا الحقل قواعـد عامـة وتوجيهـات عريضـة تتطلـب تحديـدا منضبطـاً مـن المؤسسـات التشريعيـة لـدى وضـع القوانـين الوطنيـة في هـذا الحقـل فالاتفاقيـة أرادت أن تأكـد عـلى حقيقـة أن جرائـم الكمبيوتـر والإنترنـت تنطـوي عـلى خصوصيـة في ميـدان الإثبـات والتحـري والضبـط والتفتيـش والمقاضـاة والاختصـاص، ولهـذا سـعت لتقديـم معايـير لضبـط هـذه العنـاصر مـن أجـل انسـجام الحلـول الإجرائيـة، لكنهـا منحـت هامشـا للـدول الأعضـاء لاتخـاذ تدابـير مختلفـة أو عـلى الأقـل حلـولاً بديلـة أو أخـرى غـير مـا تضمنتـه.

---

(1) Julia M. Fromholz، The European Union Data Privacy Directive، Berkeley Tech. (2000); P 22

وفي نطاق التعاون الدولي لمكافحة جرائم الكمبيوتر وضعت الاتفاقية أحكاماً تفصيلية باعتبار هذه الاتفاقية هي الأداة التشريعية الرئيسة التي ستحكم مسائل التعاون الدولي في أنشطة المكافحة، ونكتفي بالقول في هذا المقام إن أبرز ما تنطوي عليه مسائل التعاون الدولي يتمثل بالقواعد المتعلقة بتسليم المجرمين والإنابات القضائية ومسائل الضبط والتفتيش وتحريز الأدلة خارج الحدود، ولقد كانت الأحكام التي تضمنتها الاتفاقية في هذا الميدان الأكثر إثارة للجدل والتي واجهت اعتراضات واسعة من جهات عدة، ومن الواضح أن جرائم الكمبيوتر تحديدا مما لا يمكن مواجهته دون قواعد محددة تنظم المسائل الحساسة والمهمة، بل لعلها القواعد التي ستحمي السيادة الوطنية باعتبارها تنطبق على كافة الدول الأعضاء ضمن المعايير الموضوعية المقررة في الاتفاقية، وبشكل قد يحول دون تدخلات لصالح طرف دون آخر في ظل اختلال موازين القوى وسيادة إرادة المتحكمين بمصائر الشعوب والدول. [1]

ويرى الباحث أنه لأن الاتفاقية جاءت حصيلة جهود دولية وإقليمية فقد أكدت الاتفاقية على أهمية ما أنجز من جهود في حقل جرائم الكمبيوتر من قبل الأمم المتحدة ومنظمة التعاون الاقتصادي والتنمية والاتحاد الأوروبي فإن العناصر الأساسية لهذه الاتفاقية ومقوماتها هي:

الأول: يتمثل بأهمية التدابير التشريعية الموضوعية لمواجهة جرائم الكمبيوتر (نصوص التجريم الموضوعية).

الثاني: يتمثل بأهمية التدابير التشريعية الإجرامية المتلائمة مع طبيعة الكمبيوتر (النصوص الإجرائية).

الثالث: يتمثل أهمية التعاون الدولي والإقليمي في حقل مكافحة هده

(1) محمد أمين الشوابكة" جرائم الحاسوب والإنترنت الجريمة المعلوماتية" دار الثقافة للنشر والتوزيع الطبعة الأولى_الإصدار الثاني 2007 ص73.

الجرائـم والانطـلاق مـما أنجز من جهود دوليـة وإقليمية في هدا الحقل.

وبذلـك فـإن الأهـداف المسـتخلصة مـن هـذه الاتفاقيـة هـي: السـعي لتحقيـق وحـدة التدابـير التشريعيـة بـين الـدول الأوروبيـة والـدول المنظمـة للاتفاقيـة مـن غـير الـدول الأوروبيـة.

والتأكيـد عـلى أهميـة التعـاون الإقليمـي والـدولي في ميـدان مكافحـة جرائـم الكمبيوتـر والإنترنـت وإيجـاد مرجعيـة ودليـل إرشـادي للتدابـير التشريعيـة الوطنيـة في ميـدان مكافحـة جرائـم الكمبيوتـر والإنترنـت.

وضرورة فعاليـة خطـط العمـل لمكافحـة الأنشـطة التـي تسـتهدف سريـة وسـلامة وتوفـر المعلومـات وأنظمـة الكمبيوتـر وشـبكات الكمبيوتـر وأنشـطة إسـاءة اسـتخدام الكمبيوتـر والشـبكات، بمـا في ذلـك تحديـد الإطـار الموضوعـي لهـذه الأنشـطة والإطـار الإجـرائي المتصـل بالتحقيـق والتحـري والمقاضـاة في ميـدان جرائـم الكمبيوتـر عـلى المسـتوى الوطنـي والـدولي.

تحقيـق التـوازن بـين حمايـة حقـوق الإنسـان الأساسـية (المعـترف بهـا بموجـب اتفاقيـة مجلـس أوروبـا لحمايـة حقـوق الإنسـان وحريتـه الأساسـية لعـام 1950 والعهـد الـدولي للحقـوق المدنيـة والسياسـية لعـام 1966 والاتفاقيـات العالميـة الأخـرى في ميدان حقـوق الإنسـان)، وتحديـد الحقـوق المتصلـة بالـرأي وحريـة الوصـول للمعلومـات وحريـة البحـث والتلقـي والنقـل للمعلومـات والأفـكار، وبـين الحـق في الخصوصيـة وفي حيـازة المعلومـات والاسـتفادة مـن عنـاصر الملكيـة الفكريـة لهـا، ولعـل هـذا المنطلـق يمثـل النظـرة الفلسـفية الحكيمـة لظاهـرة جرائـم الكمبيوتـر ووجـوب الحمايـة منهـا دون الوصـول إلى مـدى تتأثـر فيـه حقـوق الأفـراد بالوصـول إلى المعلومـات أو تتأثـر من أنشـطة الاحتـكار والاسـتغلال غـير المـشروع للمعرفـة.

المبحث الثاني

الجرائم الإلكترونية والجريمة المعلوماتية

عندما ظهرت شبكة الإنترنت ودخلت جميع المجالات كالكمبيوتر بدءًا من الاستعمال الفردي ثم المؤسسي والحكومي كوسيلة مساعدة في تسهيل حياة الناس اليومية، انتقلت جرائم الكمبيوتر لتدخل فضاء الإنترنت، فظهر ما عرف بجرائم الإنترنت كأداة أساسية، وكما هو الحال في جرائم الحاسوب كذلك جرائم الإنترنت قد تكون الإنترنت هدفًا للجريمة أو أداة لها.

- وهنا سيتم التطرق إلى مفهوم الجريمة الإلكترونية (**المطلب الأول**).
- وأنواعها المتعلقة بالبيانات الشخصية (**المطلب الثاني**).
- وما المسؤولية القانونية لمقدمي خدمة الإنترنت (**المطلب الثالث**).

المطلب الأول

الجريمة الإلكترونية

ويقسّم باحثون متخصصون في جرائم الإنترنت تلك الجرائم ضمن فئات متعددة منها ما يتعلق بجهاز الكمبيوتر كإتلاف وتشويه البيانات والتلاعب في المعلومات المخزنة، وأخرى تتعلق بالشخصيات أو البيانات المتصلة بالحياة الخاصة، بالإضافة إلى جرائم ترتبط بحقوق الملكية الفكرية لبرامج الكمبيوتر، وانتحال شخصية أخرى بطريقة غير شرعية على الإنترنت، والمضايقة والملاحقة، والتغرير والاستدراج وهما من أشهر جرائم الإنترنت وأكثرها انتشارًا خاصة بين أوساط صغار السن من مستخدمي الشبكة.

ويتحدث الكثير منهم على أن صناعة ونشر الإباحية مما يحضُّ القصر على أنشطة جنسية غير مشروعة، وصناعة الإباحية من أشهر الصناعات الحالية وأكثرها رواجًا خاصة في الدول الغربية والآسيوية علاوة على عمليات النصب والاحتيال نظرًا لأن الإنترنت مجال رحب تمارس فيه جميع أشكال التعاملات إلا هذه الميزة شابتها سلبيات عديدة أبرزها إمكانية النصب والاحتيال بخرق هذه التعاملات.

تعتبر شبكة الإنترنت أكبر شبكة في تاريخ البشرية، وهي أحدث أدوات العالم لربط أكثر من 500 مليون حاسوب في أكثر من 200 دولة، ويستخدمها أكثر من مليار مشترك. والجريمة الإلكترونية صراع بين التقدم التقني وحماية وأمن الخصوصية privacy.

يقال إن السرقات السنوية وصلت إلى أكثر من مليوني حالة، إضافة إلى مئات الآلاف من الشركات التي وقعت ضحية القراصنة والمتلصصين، وذلك بسبب الخلل وعدم الإحكام في وسائل الأمن لدى المواقع الإلكترونية والتي يجب سدها في أقرب وقت، حيث إنه من المتوقع أن تتضاعف هذه الأرقام.

- ولتفهـم طبيعـة الجريمـة الإلكترونيـة يجـب الإجابـة عن عدة تسـاؤلات وهي ماهيـة الجريمـة الإلكترونيـة **(الفـرع الأول)**.

- ومـا الطبيعـة القانونية للجريمـة الإلكترونية **(الفرع الثاني)**.

- ومـا الفـرق بين الجريمـة الإلكترونية والجريمة المعلوماتيـة **(الفرع الثالث)**.

الفرع الأول

ماهية الجريمة الإلكترونية

يشير مصطلح الجريمة الإلكترونية إلى أي جريمة تتضمن الحاسوب أو الشبكات الحاسوبية. قد يستخدم الحاسوب في ارتكاب الجريمة وقد يكون هو الهدف.

ويمكن تعريف الجريمة الإلكترونية على أنها: أي مخالفة ترتكب ضد أفراد أو جماعات بدافع جرمي ونية الإساءة لسمعة الضحية أو لجسدها أو عقليتها، سواء كان ذلك بطريقة مباشرة أو غير مباشرة، وأن يتم ذلك باستخدام وسائل الاتصالات الحديثة مثل الإنترنت (غرف الدردشة أو البريد الإلكتروني أو المجموعات وغيرها [1]

والجريمة الإلكترونية: هي الجريمة ذات الطابع المادي، التي تتمثل في كل سلوك غير قانوني مرتبط بأي شكل بالأجهزة الإلكترونية، يتسبب في حصول المجرم على فوائد مع تحميل الضحية خسارة، ودائماً يكون هدف هذه الجرائم هو سرقة وقرصنة المعلومات الموجودة في الأجهزة، أو تهدف إلى ابتزاز الأشخاص بمعلوماتهم المخزنة على أجهزتهم المسروقة.

والجريمة الإلكترونية لها مسميات عدة منها:

1 - جرائم الحاسوب والإنترنت.

2 - جرائم التقنية العالية.

(1) Moore، R. "Cyber crime: Investigating High - Technology Computer Crime،" Cleveland، Mississippi: Anderson Publishing (2005) P.143

و أيضا نضال الشاعر"، الاجرام المعلوماتي في وسائل الاتصال الالكتروني"، دراسة منشورة في نشرة المعلومات القانونية الصادرة عن جمعية علماء المعلوماتية في لبنان، العدد 3 آيار 2005، دار ناشرون، بيروت 2005، ص:4.

3 - الجريمـة الإلكترونية.

4 - الجريمة السـايْبرِيّة.

5 - جرائـم أصحـاب الياقات البيضاء.

وقـد تتنـوع أعـمار منفـذي الجرائـم الإلكترونيـة مـع اختـلاف دوافعهـم، فهنـاك مـن منفـذي الهجـمات الأطفـال والمراهقـين الذيـن تكـون في الغالـب دوافعهـم لمجـرد التسـلية غـير مدركـين حجـم الأضرار التـي يقومـون بهـا، وهنـاك المحترفـين والمختصـين والإرهابيـين الذيـن مـن الممكـن أن تحطـم أعمالهـم شركات ضخمة وتضر بـدول كبيرة.[1]

ويمكـن إيجاز أهداف الجريمـة الإلكترونية في:

التمكـن مـن الوصـول إلى المعلومـات بشـكل غـير شرعـي، كسرقـة المعلومـات أو الاطـلاع عليهـا أو حذفهـا أو تعديلهـا بمـا يحقـق هـدف المجـرم، التمكـن مـن الوصـول عـن طريـق الشـبكة العنكبوتيـة إلى الأجهـزة الخادمـة الموفـرة للمعلومـات وتعطيلهـا، و الحصـول عـلى المعلومـات السريـة للجهـات المسـتخدمة للتكنولوجيا كالمؤسسـات والبنـوك والجهـات الحكوميـة والأفـراد وابتزازهـم بواسـطتها وكذلـك الكسـب المـادي أو المعنـوي أو السـياسي غـير المـشروع عـن طريـق تقنيـة المعلومـات مثـل عمليـات اخـتراق وهـدم المواقـع عـلى الشـبكة العنكبوتيـة وتزويـر بطاقـات الائتـمان وسرقـة الحسـابات المصرفيـة.[2]

---

(1) د. محمد سامي الشوا - ثورة المعلومات وانعكاساتها على قانون العقوبات - دار النهضة العربية - القاهرة - 1994 - ص2).173 راجع أيضا د. هدى حامد قشقوش - جرائم الحاسب الإلكتروني في التشريع المقارن - دار النهضة العربية - القاهرة - 1992 - ص9). وأيضا محمد حسام، محمود لطفي، "الحماية القانونية لبرامج الحاسب الالكتروني" دار الثقافة للطباعة والنشر القاهرة، الطبعة الأولى 1978، ص 161

(2) محمد حسام، محمود لطفي، "الحماية القانونية لبرامج الحاسب الإلكتروني" دار الثقافة للطباعة والنشر القاهرة، الطبعة الأولى 1978، ص 161. و راجع أيضا جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالإنترنت، دار النهضة العربية، القاهرة 1998م ص 75.

تعرف الجريمة بأنها الجريمة والارتكاب المتعمد لفعل ضار من الناحية الاجتماعية أو فعل خطير محظور يعاقب عليه القانون.

وتمثل الجرائم الإلكترونية مجموعة الأفعال والأعمال غير القانونية التي تتم عبر معدات أو أجهزة إلكترونية أو شبكة الإنترنت أو تبث عبرها محتوياتها.

وهي ذلك النوع من الجرائم التي تتطلب الإلمام الخاص بتقنيات الحاسب الآلي ونظم المعلومات لارتكابها أو التحقيق فيها ومقاضاة فاعليها.[1]

وقد يتم تصنيف الجرائم الإلكترونية تبعا لدور الكمبيوتر في الجريمة بالجرائم التي تستهدف عناصر (السرية والسلامة)، ومنها الدخول غير الشرعي والاعتراض غير القانوني وكذلك تدمير البيانات بمسحها أو تعطيلها أو تشويهها وجعلها غير قابلة للاستخدام.

ويمكن تصنيفها أيضا من حيث إساءة استخدام الأجهزة مثل الجرائم المرتبطة بالحاسب مثل التزوير، الاحتيال، وقرصنة البرمجيات كالإخلال بحقوق المؤلفين [2]

(1) عبد الفتاح مراد، شرح جرائم الكمبيوتر والإنترنت، دار الكتب والوثائق المصرية، ص 38.

(2) د. جميل عبد الباقي الصغير - المواجهة الجنائية لقرصنة البرامج التلفزيونية المدفوعة - دار النهضة العربية - القاهرة - 2001 - ص2).11 وراجع أيضاً. هلال عبد اللاه احمد - التزام الشاهد بالإعلام في الجرائم المعلوماتية - ط1 - دار النهضة العربية - القاهرة - 1997 - ص6)

الفرع الثاني

الطبيعة القانونية للجريمة الإلكترونية

يتمحور الحديث عن الطبيعة القانونية للجريمة الإلكترونية حول الوضع القانوني للبرامج والمعلومات، وهل لها قيمة في ذاتها أم أن قيمتها تتمثل في أنها مجموعة مستحدثة من القيم القابلة للاستثناء يمكن الاعتداء عليها بأية طريقة كانت، لذلك انقسم الفقه اتجاهين:

الأول: يرى أنه وفقا للقواعد العامة أن الأشياء المادية وحدها هي التي تقبل الحيازة والاستحواذ، وأن الشيء موضوع السرقة يجب أن يكون ماديا أي له كيان مادي ملموس حتى يمكن انتقاله وحيازته عن طريق الاختلاس المكون للركن المادي في جريمة السرقة، ولما كانت المعلومة لها طبيعة معنوية ولا يمكن اعتبارها من قبيل القيم القابلة للحيازة والاستحواذ، إلا في ضوء حقوق الملكية الفكرية، لذلك تستبعد المعلومات ومجرد الأفكار من مجال السرقة، ما لم تكن مسجلة على إسطوانة أو شريط، فإذا ما تم سرقة إحدى هاتين الدعامتين الخارجية، فلا تثور مشكلة قانونية في تكييف الواقعة على أنها سرقة مال معلوماتي ذا طبيعة مادية، وإنما المشكلة تثور عندما نكون أمام سرقة مال معلوماتي غير مادي.

والاتجاه الثاني: يرى المعلومات ما هي إلا مجموعة مستحدثة من القيم قابلة للاستحواذ مستقلة عن دعامتها المادية، على سند من القول إن المعلومات لها قيمة اقتصادية قابلة لأن تحاز حيازة غير مشروعة.[1]

(1) Williams، M. "Virtually Criminal: Crime، Deviance and Regulation Online"، Routledge، London (2006) P.175

عمرو أحمد حسبو – حماية الحريات في مواجهة نظم المعلومات - دار النهضة العربية – القاهرة - 1985 - ص3.

وعلى الصعيد نفسه ثمة من يقول إنه يجب أن نفرق بأن هناك مالاً معلوماتيا ماديّا فقط، ولا يمكن أن يخرج عن هذه الطبيعة وهي آلات وأدوات الحاسب الآلي مثل وحدة العرض البصري ووحدة الإدخال، وأن هناك من المال المعلوماتي المادي ما يحتوي على مضمون معنوي هو الذي يعطيه القيمة الحقيقية وهي المال المادي الشريط الممغنط أو الاسطوانة الممغنطة أو الذاكرة أو الأسلاك التي تنتقل منها الإشارات عن على بعد، كما هو الحال في جرائم التجسس عن بعد، إذن من المنطق القول إذا حدثت سرقة فإنه لا يسرق المال المسجل عليه المعلومة والبرامج لقيمته المادية وهي ثمن الشريط أو ثمن الإسطوانة، وإنما يسرق ما هو مسجل عليهما من معلومات وبرامج.[1]

ويرى أصحاب هذا الرأي أن التحليل المنطقي يفرض الاعتداد بفكرة الكيان المادي للشيء الناتج عنه اختلاس المال المعنوي البرامج والمعلومات، وأنها لا يمكن أن تكون شيئا ملموسا محسوسا، ولكن لهما كيان مادي قابل للانتقال والاستحواذ عليه بتشغيل الجهاز ورؤيتهما على الشاشة مترجما إلى أفكار تنتقل من الجهاز إلى ذهن المتلقي، وانتقال المعلومات يتم عن طريق انتقال نبضات ورموز تمثل شفرات يمكن حلها إلى معلومات معينة لها أصل صادر عنه يمكن سرقته، وبالتالي لها كيان مادي، يمكن الاستحواذ عليه (البرامج والمعلومات)، واستطرد أصحاب هذا الاتجاه في القول بأنه طالما أن موضوع الحيازة (أي المعلومات) غير مادي، فإن واقعية الحيازة تكون من نفس الطبيعة أي غير مادية (ذهنية)، وبالتالي يمكن حيازة المعلومات بواسطة الالتقاط الذهني عن طريق البصر[2].

وردا على قول الرافضين لملكية الغير للشيء المعلوماتي بأن البرنامج

---

(1) د.هشام محمد فريد رستم - الجرائم المعلوماتية - أصول التحقيق الجنائي الفني واقتراح بإنشاء آلية عربية موحدة للتدريب التخصصي - بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت - في (3 - 1 مايو 2000م. - ص 49.

(2) د. محمد على العريان، الجرائم المعلوماتية، دار الجامعة الجديدة للنشر، الإسكندرية، 2004 ص107

والمعلومة من نوع الخلق الفكري ذاته الذي ليس ملكا لأحد، قال أصحاب هذا الرأي إن البرنامج من الناحية القانونية تعتبر ملكا لمن ابتكرها، وإن التحليل المنطقي لا يمكنه إنكار ملكية شخص ما للبرنامج والمعلومة، ومن ثم فهي ليست ملكا للسارق، بل هو يقوم بالاستحواذ على شيء ليس مملوكا له.

واستشهد أنصار هذا الاتجاه بما توصلت إليه محكمة النقض المصرية فيما يتعلق بسرقة الكهرباء، فهي أيضا مال غير ملموس، وحسمها هذا كان مبنيا على اعتبار التيار الكهربائي وإن كان ليس مالا ملموسا، فله كيان مادي متمثل في الأسلاك والتوصيلات التي تمر من خلالها، وبالتالي يمكن اختلاسه وانطباق نص السرقة عليه[1]، وكانت محكمة النقض المصرية قد حذت حذو محكمة النقض الفرنسية في حكمها بإمكانية سرقة التيار الكهربائي، وكذلك ما ذهبت إليه في شأن سرقة خط الهاتف من أنه وإن لم يكن مالا ماديا ملموسا، فإنه قابل للحيازة والانتقال.

وذهب أصحاب هذا الاتجاه في تحليله لإمكانية التشابه بين سرقة المال المعلوماتي المعنوي وسرقة التيار الكهربائي إلى القول بأنه رغم أن القضاء قد اعتبر التيار الكهربائي شيئا قابلا للسرقة، إلا أنه ليس للتيار الكهربائي نفس مادية الأشياء الملموسة، معولا في هذا الرأي على تحليله بأن كلمة (هي) ليست مرتبطة بكلمة مادي، ولا يمكن أن تعطي تكييفا مساويا لكلمتي شيء ومادي، وبالتالي فإن البرنامج والمعلومة شيء تدخل ضمن نطاق الأشياء وليس حتما ضمن الماديات، وهذا ما يؤكده الفقيه (Vitu) ؛ وأضاف هذا الاتجاه أن تعريف كلمة شيء تعني كل حقيقة ملموسة ماديا أو معنويا، وأن استخدام المشرع الفرنسي لكلمة شيء لا تقصر الأشياء على الماديات، بل تمتد لأشياء لتشمل ما قد يكون مجردا معنويا، ودلل على تصور تطبيق نص السرقة

---

(1) حكم نقض إبريل 1931، مجموعة القواعد ج 2، رقم 324. كذلك 8 ديسمبر 1952 مجموعة الأحكام س 24 رقم 81 ص255.

على المعلومات بأن أورد حكما للقضاء الفرنسي في قضية Loqabax أدانت بمقتضاه المحكمة متهما كان يعمل موظفا قام بتصوير مستندات سرية ضد رغبة من يعمل لديه، على سرقة المعلومات المدونة بالورقة وليس على سرقته للورقة ذاتها. (1)

ونعتقد أن المشرع الليبي أحسن حينما تدخل وحسم الجدل الفقهي والتردد في التطبيقات القضائية بأن أردف فقرة ثانية إلى المادة 444 من قانون العقوبات المتعلقة بالسرقة نص فيها: "ويعد من الأموال المنقولة في حكم قانون العقوبات الطاقة الكهربائية وجميع أنواع الطاقة ذات القيمة الاقتصادية "(2).

وقد حان الآن الوقت لتدخله لمواجهة الجرائم الإلكترونية بالنص على تجريم الاعتداء على المال المعلوماتي المعنوي سواء بالنص على كل جريمة على حده كما فعل المشرع الفرنسي في القانون الجديد، أو أن يقرر التجريم بنص واحد، يشمل بالحماية الجنائية كل صور الاعتداء، السرقة أو الإتلاف أو غيرهما، والحل الأخير نراه الأنسب تجنبا لما وقع فيه المشرع الفرنسي من تقصير وعدم شمولية حينما نص على حماية محل جريمة الإتلاف وتجاهل محل جريمة السرقة، وقد يحسب للمشرع الفرنسي محاولته - التي لم يكتب لها النجاح - تعديل قانون العقوبات الجديد بالنص على تجريم سرقة المال المعلوماتي المعنوي المتمثل في البرامج والمعلومات، وذلك في نص المادة 1/307 الذي استعمل فيه كلمة التقاط (Capter) لتعبر عن الاختلاس، حيث نص على أن:" كل من التقط بطريق الاختلاس والتحايل برنامجا أو معلومات أو أي عنصر من عناصر نظام المعالجة الآلية للبيانات يعاقب......"

---

(1) عمرو أحمد حسبو المرجع السابق ص 22.

(2) الجريمة الإلكترونية والتغلب على تحدياتها، ورقة مقدمة من:د. مفتاح بوبكر المطردي، المستشار بالمحكمة العليا الليبية إلي المؤتمر الثالث لرؤساء المحاكم العليا في الدول العربية بجمهورية السودان المنعقد في 23 - 25 / 9 / 2012 ص24.

ومـن هنـا نخلـص بـأن التسـليم بأن المـال المعلوماتي المعنـوي غير قابل للاسـتحواذ وليـس مـالا، وبالتـالي غـير قابـل للسرقـة سـيؤدي إلى تجريـده مـن الحمايـة القانونيـة الجنائيـة ويفتـح المجـال واسـعا أمـام مجرمـي وقراصنـة البرامـج والمعلومـات.

الفرع الثالث

مفهوم الجريمة المعلوماتية

يصعب الاتفاق على تعريف موحد للجريمة المعلوماتية، حيث اختلفت الاجتهادات في ذلك اختلافاً كبيرا، يرجع إلى سرعة وتيرة تطور التقنية المعلوماتية من جهة، وتباين الدور الذي تلعبه هذه التقنية في الجريمة من جهة أخرى، فالنظام المعلوماتي لهذه التقنية يكون محلاً للجريمة تارة، ويكون وسيلة لارتكابها تارة أخرى، فكلما كان البحث منصباً على الجرائم التي ترتكب ضد النظام المعلوماتي انطلق التعريف من زاوية محل الجريمة بأنها الجريمة المرتكبة بالاعتداء على النظام المعلوماتي، أما إذا كان البحث منصباً على دراسة الجرائم التي ترتكب باستخدام التقنية المعلوماتية ارتكز التعريف على الوسيلة وكان:" كأشكال السلوك غير المشروع الذي يرتكب باستخدام الحاسب الآلي.

تجدر الإشارة أيضاً إلى أن أهم عوامل صعوبة الاتفاق على تعريف هو أن التقنية المعلوماتية أصبحت تحل محل العديد من التقنيات السابقة كالهاتف والفاكس والتلفزيون، فالمسألة لم تقتصر على معالجة البيانات فحسب بل تعدتها إلى وظائف عديدة مثل وظيفة النشر والنسخ، وهو ما يحتم ضرورة التفرقة بين جرائم الإنترنت وشبكات المعلومات بالمعنى الفني عن بقية الجرائم الأخرى التي يستخدم فيها الإنترنت أو الحاسب الآلي كأداة لارتكابها.

فهناك العديد من التعريفات للجريمة المعلوماتية منها:

أولا: أنها أية جريمة ضد المال مرتبطة باستخدام المعالجة الآلية للمعلومات[1].

---

(1) D.B. parker "Combattre la crimpinalite in formatiqe" (1985) p.18

ثانيا: الاعتداءات القانونية التي ترتكب بواسطة المعلوماتية بغرض تحقيق ربح[1].

ثالثا: مجموعة من الأفعال المرتبطة بالمعلوماتية التي يمكن أن تكون جديرة بالعقاب.[2]

رابعا: مجموعة الجرائم المتصلة بعلم المعالجة المنطقية للمعلومات[3].

يتضح بجلاء أن التعاريف الأخيرة أكثر منطقية من سابقتها لمحاولتها استبعاد الأفعال الإجرامية التي ترتكب بمناسبة الاستخدام العارض للحاسب الآلي فضلا عن استبعاد الباعث أو الغاية من القيام بتلك الأفعال، ومنها تحقيق الربح وعلى ذلك يمكن القول إن الجرائم المعلوماتية الواقعة ذات طبيعة قانونية خاصة تميزها عن غيرها من الجرائم التقليدية فضلا عن الخصائص والمميزات الأخرى المترتبة عليها.

فيقصد بجرائم المعلوماتية الدخول غير المشروع إلى الشبكات الخاصة كالشركات والبنوك وغيرها وكذلك الأفراد، والعبث بالبيانات الرقمية التي تحتويها شبكة المعلومات مثل تزييف البيانات أو إتلافها ومحوها، وامتلاك أدوات أو كلمات سرية لتسهيل ارتكاب مثل هذه الجرائم التي تلحق ضرراً بالبيانات والمعلومات ذاتها وكذلك بالنسبة للبرامج والأجهزة التي تحتويها وهي الجرائم التي تلعب فيها الفنية المعلوماتية دوراً رئيساً في مادياتها أو السلوك الإجرامي فيها. [4]

---

(1) سعد الحاج بكري - شبكات الاتصال وتوظيف المعلومات في مكافحة الجريمة - المجلة العربية للدراسات الأمنية والتدريب - س 6 - ع 11..92 - الرياض - 1990 ص45.

(2) Vivant et lestanc" lamy in Droit de Linformatique" paris (1989) P.45

(3) د. هدى حامد قشقوش - جرائم الحاسب الإلكتروني في التشريع المقارن - دار النهضة العربية - القاهرة - 1992 ص56.

(4) د.هشام فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات حديثة، أسيوط،1992 ص46. وراجع أيضا - محمد أمين الرومي، جرائم الكومبيوتر والإنترنت، دار المطبوعات الجامعية 2003.

ويرى الباحث أن الجرائم المعلوماتية لها أنواع وأصناف عديدة، وكما أسلفنا القول فإن الجريمة المعلوماتية تتميز بأنها تضم نوعين من الجرائم المستحدثة:

الأول: أنواعاً مستحدثة من الاعتداء على مصالح محمية جنائياً بالنصوص القانونية التقليدية، أي أن في هذه الحالات فإن طرق الاعتداء فقط هي المستحدثة لأنها تتم عن طريق التقنية المعلوماتية بعد أن كانت ترتكب بالسلوك المادي الملموس، أما محل الاعتداء فهي المصالح المحمية أصلا حماية جنائية على مر الأزمان والعصور كالأموال والشرف والاعتبار.

أما النوع الثاني: فيضم أنواعاً أخرى من الاعتداءات بالطرق المستحدثة على مصالح مستحدثة لم تعرفها القواعد التقليدية كالشبكات المعلوماتية التي تتعرض للاختراق أو التعطل أو الإغراق.

أولاً: الركن المادي في الجرائم المعلوماتية عبر الإنترنت:

إن النشاط أو السلوك المادي في جرائم الإنترنت يتطلب وجود بيئة رقمية واتصال بالإنترنت ويتطلب أيضا معرفة بداية هذا النشاط والشروع فيه ونتيجته. فمثلا يقوم مرتكب الجريمة بتجهيز الحاسب لكي يحقق له حدوث الجريمة.

فيقوم بتحميل الحاسب ببرامج اختراق، أو أن يقوم بإعداد هذه البرامج بنفسه، وكذلك قد يحتاج إلي تهيئة صفحات تحمل في طياتها مواد داعرة أو مخلة بالآداب العامة وتحميلها علي الجهاز المضيف Hosting Server، كما يمكن أن يقوم بجريمة إعداد برامج فيروسات تمهيداً لبثها.[1]

(1) Brent E. Turvey، Diana Tamlyn، Jerry Chisum Criminal Profiling: An Introduction to Behavioral Evidence Analysis،، 1 edition، Academic Press Limited 1999.P 56

ليس كل جريمة تستلزم وجود أعمال تحضيرية، وفي الحقيقة يصعب الفصل بين العمل التحضيري والبدء في النشاط الإجرامي في جرائم الكمبيوتر والإنترنت - حتى ولو كان القانون لا يعاقب علي الأعمال التحضيرية - إلا أنه في مجال تكنولوجيا المعلومات الأمر يختلف بعض الشيء. فشراء برامج اختراق، ومعدات لفك الشفرات وكلمات المرور، وحيازة صور دعارة للأطفال فمثل هذه الأشياء تمثل جريمة في حد ذاتها.[1]

تثير مسألة النتيجة الإجرامية في جرائم الإنترنت مشاكل عدة، فعلي سبيل المثال مكان وزمان تحقق النتيجة الإجرامية.

فلو قام أحد المجرمين في أمريكا اللاتينية باختراق جهاز خادم Server أحد البنوك في الإمارات، وهذا الخادم موجود في الصين فكيف يمكن معرفة وقت حدوث الجريمة هل هو توقيت بلد المجرم أو توقيت بلد البنك المسروق أو توقيت الجهاز الخادم في الصين، ويثور أيضا إشكاليات القانون الواجب التطبيق في هذا الشأن. حيث إن هناك بعد دولي في هذا المجال[2].

ثانياً: الركن المعنوي في الجرائم المعلوماتية عبر جرائم الإنترنت.

الركن المعنوي هو الحالة النفسية للجاني، والعلاقة التي تربط بين ماديات الجريمة وشخصية الجاني، وقد تنقل المشرع الأمريكي في تحديد الركن المعنوي للجريمة بين مبدأ الإرادة ومبدأ العلم. فهو تارة يستخدم الإرادة كما هو الشأن في قانون العلامات التجارية في القانون الفيدرالي الأمريكي، وأحيانا أخري أخذ بالعلم كما في قانون مكافحة الاستنساخ الأمريكي.[3]

---

(1) الدكتوره هدى قشقوش، جرائم الحاسب الإلكتروني في التشريع المقارن، الطبعة الأولى دار النهضة العربية، القاهرة، 1992، ص 20.

(2) Laura E. Quarantiello Cyber Crime: How to Protect Yourself from Computer Criminals، Tiare Publications، 1996.

(3) Ulser Sieber، legal aspects of computer related crimes، Eu Commission 1998، P 43

برزت تلك المشكلة في قضية موريس الذي كان متهما في قضية دخول غير مصرح به علي جهاز حاسب فيدرالي وقد دفع محامي موريس علي انتفاء الركن المعنوي، الأمر الذي جعل المحكمة تقول:" هل يلزم أن يقوم الادعاء بإثبات القصد الجنائي في جريمة الدخول غير المصرح به، بحيث تثبت نية المتهم في الولوج إلي حاسب فيدرالي، ثم يلزم إثبات نية المتهم في تحدي الحظر الوارد علي استخدام نظم المعلومات في الحاسب وتحقيق خسائر، ومثل هذا الأمر يستدعي التوصل إلي تحديد أركان جريمة الدخول دون تصريح ". وبذلك ذهبت المحكمة إلي تبني معيارين هنا هما الإرادة بالدخول غير المصرح به، وكذا معيار العلم بالحظر الوارد علي استخدام نظم معلومات فيدرالية دون تصريح.[1]

أما بالنسبة للقضاء الفرنسي فإن منطق سوء النية هو الأعم في شأن جرائم الإنترنت، حيث يشترط المشرع الفرنسي وجود سوء نية في الاعتداء علي بريد إلكتروني خاص بأحد الأشخاص. هذا ويمكن القول أيضا بتوافر الركن المعنوي في جرائم الإنترنت في المثال التالي، قيام أحد القراصنة بنسخ برامج كمبيوتر من موقع علي شبكة الإنترنت، والقيام بفك شفرة الموقع وتخريبه للحصول علي البرمجيات ولإيقاع الأذى بالشركة.[2]

---

(1) محمد محيي الدين عوض – مشكلات السياسة الجنائية المعاصرة في جرائم نظم المعلومات (الكمبيوتر) – ورقة عمل مقدمة إلى المؤتمر السادس للجمعية المصرية للقانون الجنائي – المنعقد بالقاهرة في الفترة من 25 - 28 أكتوبر 1993 م.

(2) Donn B. Parker Fighting Computer Crime: A New Framework for Protecting Information،، 1 edition، John Wiley & Sons 1998.p 153

الفرع الثالث

المسؤولية الجنائية في الجرائم المعلوماتية والجرائم المرتكبة عبر الإنترنت

إن الوصول للمجرم المعلوماتي أو الإلكتروني يشكل عبئا فنيا وتقنيا بالغا علي القائمين بأعمال التتبع والتحليل لملابسات الوقائع الإجرامية المختلفة. وقد نصت المادة 12 من معاهدة بودابست لمكافحة جرائم القضاء المعلوماتي[1]

والتي لم تكن الولايات المتحدة طرفا فيها، وسارعت بالانضمام إليها بعد أحداث الحادي عشر من سبتمبر - تنص علي:

1 - سوف يتبنى كل طرف تدابير تشريعية، وأي تدابير أخري لضمان قيام مسؤولية الأشخاص المعنوية عن أي جريمة موصوفة في

(1) The Convention on Cybercrime، also known as the Budapest Convention on Cybercrime or the Budapest Convention، is the first international treaty seeking to address Internet and computer crime by harmonizing national laws، improving investigative techniques، and increasing cooperation among nations. It was drawn up by the Council of Europe in Strasbourg، France، with the active participation of the Council of Europe›s observer states Canada and Japan. The Convention and its Explanatory Report was adopted by the Committee of Ministers of the Council of Europe at its 109th Session on 8 November 2001. It was opened for signature in Budapest، on 23 November 2001 and it entered into force on 1 July 2004. As of March 2014، 42 states have ratified the convention، while a further 11 states had signed the convention but not ratified it. On 1 March 2006 the Additional Protocol to the Convention on Cybercrime came into force. Those States that have ratified the additional protocol are required to criminalize the dissemination of racist and xenophobic material through computer systems، as well as threats and insults motivates by racism or xenophobia.

هـذه المعاهـدة إذا مـا ارتكبـت لصالـح الشـخص المعنوي بواسـطة شـخص طبيعـي اقترفهـا بشـكل منفـرد أو بوصفـه جـزءا مـن عضـو في الشـخص المعنـوي عـلي أسـاس من:

- تفويض من الشـخص المعنوي.
- سـلطة اتخاذ قرارات لصالح الشـخص المعنوي.
- سـلطة لممارسـة رقابة أو سـيطرة داخل الشخص المعنوي.

2 - إلي جانـب الحـالات الـواردة في البنـد 1[1] سـوف يتخـذ كل طـرف التدابـير اللازمـة لضـمان قيـام مسـؤولية الشـخص المعنـوي إذا مـا أدي نقـص الإشراف أو السـيطرة مـن قبـل الشـخص الطبيعي المشـار إليـه في الفقرة 1 إلي إمكانيـة ارتـكاب جريمـة قائمـة طبقـا لهـذه المعاهـدة لصالـح الشـخص المعنـوي بواسـطة شـخص طبيعـي اقترفهـا تحـت سـيطرته.

3 - هـذه المسـؤولية لـن تؤثر عـلي قيام المسـؤولية الجنائيـة للأشـخاص الطبيعيين الذين اقترفـوا الجريمة.

(1) Convention on Cybercrime، Budapest، 23 November 2001. on the website of the Council of Europe

المطلب الثاني

نماذج من الجرائم المعلوماتية التي تمس البيانات الشخصية

- تتنوع الجرائم الإلكترونية التي تمس البيانات الشخصية فمنها (جريمة المعالجة الإلكترونية)**(الفرع الأول)**.
- جريمة الإفشاء غير المشروع للبيانات **(الفرع الثاني)**.
- وجريمة الانحراف عن الغرض أو الغاية من المعالجة الإلكترونية**(الفرع الثالث)**.
- وأخيراً جريمة قرصنة البريد الإلكتروني **(الفرع الرابع)**.

الفرع الأول

جريمة المعالجة الإلكترونية

على الرغم من اعتراف بعض الدول بمبدأ حرية الاتصال ونقل المعلومات فإنها قد تأخذ بنظام الترخيص وبمقتضاه يلزم صدور ترخيص سابق بإقامة أو استعمال المنشآت والأجهزة التي تستخدم في بث أو نقل المعلومات أو معالجتها وتسمى بعقود نقل التكنولوجيا أي أن من حق صاحب البرنامج التصرف في البرنامج واستغلاله واستعماله.

وفي الغالب أن يتنازل صاحب البرنامج عن حقوقه المتفرعة عن الملكية كلها أو بعضها للغير بيعها أو بمنح ترخيص باستغلالها وتبقى له جميع حقوق المؤلف التي يحميها حق المؤلف إذ لا يتلقى غير السوي النسخة المادية للبرنامج ولكن إذا تلقى الغير ملكية هذه النسخة أو الحق في استغلالها فإن له الحق في استخدامها في تشغيل الحاسوب بغرض معالجة المعلومات ونقلها داخل الدولة أو خارجها عن طريق شبكات الاتصال، ووفقا للشروط التي بمقتضاها تلقى ملكية البرنامج أو الحق في استغلاله.

وعليه يمكن بيان معالم هذه الجريمة من خلال بحث أركانها ومن ثم بيان عقوبتها على النحو الآتي:

أولا: الركن المادي:

يتخذ الركن المادي في هذه الجريمة صورة السلوك، وهو قيام الجاني بفعل يتمثل بالمعالجة الإلكترونية للبيانات الشخصية [1] التي تشمل مجموعة العمليات التي تتم إلكترونيًا بواسطة استخدام الحاسوب والمتعلقة بعمليات التسجيل والتعديل والإضافة والمحو أو أي تغيير آخر يمكن أن يطرأ على

(1) المادة (41) من قانون المعالجة الإلكترونية والحريات الفرنسي رقم (17) لسنة 1978).

هــذه البيانــات ســواء كانــت عمليــات فــرز أم حفــظ أم أيــة عمليــة مــن ذات الطبيعــة تحمــل معالجــة لهــذه البيانــات بقصــد الربــط بينهــا للحصــول عــلى المعلومــات، وعليــه فالمعالجــة الإلكترونيــة تشــمل:

أ - عمليـات التغيير:

وهـي التعديـل والإضافـة أو المونتـاج أو الفـرز والتصنيـف أو الجدولـة فضـلا عن عمليـات المحـو الجـزئي لاسـتكمال متطلبـات التعديـل والمونتاج

ب - عمليـات الحـذف والمحو الـكلي لهذه البيانات.

وتكـون طريقـة المعالجـة الإلكترونيـة إمـا بالالتـماس المبـاشر مـع الحاسـوب الذي يحتـوي عـلى البيانـات الشـخصية أو أن تتـم المعالجـة عـن بعـد باسـتخدام الشـبكات للحصـول عـلى اتصـال غـير مـشروع يمكن المسـتخدم بعـد اخـتراق أنظمة الأمـن والحماية لهـذه الحواسـيب مـن معالجـة البيانـات الشـخصية[1] .

فالمقصـود بعمليـات التغيـير هـي كل العمليـات التـي تتـم باسـتخدام الحاسـوب التـي تـؤدي إلى تحويـل الملامـح الأصليـة الشـخصية التابعـة لشـخص معـين وتشـمل عمليـات المعالجـة أيضـا عمليـات الحـذف الـكلي لهـذه البيانـات أو عـلى عمليـات التسـجيل والحفـظ، وعليـه يتوافـر الركـن المـادي لهـذه الجريمـة بمجـرد معالجـة البيانات دون ترخيـص حتـى وإن لم يترتـب عـلى ذلـك أيـة نتيجـة إجراميـة، فالجريمـة تعـد جريمة سـلوكية لا تتطلـب تحقيـق نتيجـة معينـة.[2]

ثانيا:الركـن المعنوي:

ويتخـذ صـورة القصـد الجنـائي وهـو مسـتفاد مـن طبيعـة الأفعـال التـي تقـوم

---

(1) د. عمرو أحمد حسبو - حماية الحريات في مواجهة نظم المعلومات - دار النهضة العربية - القاهرة - 1985 - ص 125)..(6) المادة (41) من قانون المعالجة الإلكترونية والحريات الفرنسي لسنة 1978) ص123.

(2) د. عبد الأحد جمال الدين - النظرية العامة للجريمة - دار الثقافة الجامعية - القاهرة - 1996ص34.

بها الجريمة، ويقوم القصد الجنائي هنا على عنصرين هما: العلم والإرادة. فالعلم يعني علم الجاني بالصفة الاسمية أو الشخصية للبيانات، وأن يعلم أن من طبيعة الحاسوب الإلكترونية إجراء المعالجة الإلكترونية لهذه البيانات دون ترخيص من اللجنة المختصة بذلك.

أما الإرادة فهي أن تتجه إرادة الجاني إلى إجراء المعالجة الإلكترونية لهذه البيانات بأية صورة كانت أي بالمخالفة لاتخاذ الإجراءات الأولية لإجراء المعالجة الإلكترونية للبيانات،[1] أي أن القصد المتطلب لقيام هذه الجريمة هو القصد العام ولا عبرة بالبواعث التي دفعت الجاني إلى ارتكاب فعله فسواء كان الباعث هو الإضرار المادي بالشخص أم استغلال هذه البيانات للإساءة إلى سمعة الشخص أو لمجرد الفضول وحب الاستطلاع.[2]

(1) . د. محمد عبد اللطيف عبد العال - الجرائم المادية وطبيعة المسؤولية الناشئة عنها - دار النهضة العربية - القاهرة - 1997، ص120.

(2) Alain Bensoussan، Internet، aspects juridiques، éd. Hermes، 1998 P116 ؛

الفرع الثاني

جريمة الإفشاء غير المشروع للبيانات

على الرغم من تعدد بنوك المعلومات وكثرة المعلومات أو البيانات المخزونة غير أن تلك البيانات تحظى بحرمة وقدسية كباقي صور الخصوصية، فقد تشمل الأسرار الشخصية أو الأوضاع الذاتية في مختلف الاتجاهات والحفاظ عليها من العلن مهمة ذات طابع إنساني، وقد جسد المشرع الفرنسي هذه ا لحماية للبيانات أيا كان نوعها من الإفشاء والنقل والنشر ثم تحريم كل فعل يرتكبه شخص من شأنه الكشف عن بيانات شخصية بمناسبة تسجيل أو نقل أو أي شكل من أشكال معالجة البيانات الشخصية التي يترتب على كشفها الاعتداء على الشخصية الاعتبارية لصاحب الشأن أو حرمة حياته الخاصة في هذه المعلومات دون تصريح بذلك من صاحب الشأن للغير الذي لا توجد له أية صفة في تلقي هذه المعلومات. وعليه لكي تقوم هذه الجريمة يتعين توافر ركنين هما:

أولا: الركن المادي:

ويتخذ صورة السلوك بالقيام بأحد الفعلين هما فعل الحيازة للبيانات وفعل الإفشاء لها وفي الفعل الأول يستوي لدى القانون أن يكون حيازة البيانات بقصد تصنيفها أو نقلها أو لعلاجها تحت أي شكل من الأشكال أما الفعل الثاني فهو فعل إفشاء هذه البيانات للغير أي إلى شخص آخر غير مختص أو مخول بتلقي هذه المعلومات أو البيانات.[1]

---

(1) د.عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والإنترنت في القانون العربي النموذجي، ط1، دار الفكر الجامعي، الإسكندرية، 2006. ص 118.

وفضلا عما تقدم ينبغي لقيام الركن المادي تحقق النتيجة الإجرامية وهي أن يترتب على فعل الإفشاء إضرار للشخص أو اعتداء على حرمة خصوصيته أو شرفه أو اعتباره وأن ترتبط هذه النتيجة بالفعل بعلاقة سببية بمعنى أنه إذا لم يترتب على فعل الإفشاء اعتداء على كرامة الشخص أو اعتباره أو حرمة خصوصيته فإنه لا تتوافر عناصر الركن المادي، ومن ثم لا تقوم هذه الجريمة، وعليه يتطلب لقيام الركن المادي في هذه الجريمة ثلاثة شروط هي:

١ - أن يكون من طبيعة فعل الإفشاء اعتداء على الشرف أو الحياة الخاصة كما يستوي في نظر القانون أن تكون هذه البيانات صحيحة أو مزورة طالما أن إفشاءها يمثل اعتداء ولا يشترط طريقة معينة في الحصول على هذه البيانات إذ أن العبرة في الحصول عليها أو معالجتها عن طريق وسيلة معالجة إلكترونية وهو الحاسوب الذي تخزن وتعالج فيه المعلومات[1]

٢ - انتفاء رضاء المجني عليه.

3 - أن يكون الإفشاء من شخص أو أشخاص ليس له أو لهم الحق بالاطلاع على هذه البيانات.

ثانيا: الركن المعنوي:

يختلف الركن المعنوي لهذه الجريمة عن سابقه إذ يتخذ إحدى الصورتين، إما العمد أو الخطأ.

فالصورة الأولى: القصد الجنائي أو العمد وتتمثل بعنصري العلم

(1) أسامة احمد - جرائم الحاسب الآلي والإنترنت - ط ١ - دار وائل للنشر - الأردن - 2001 ص43 راجع أيضا د. عفيفي كامل عفيفي، جرائم الكمبيوتر ودور الشرطة والقضاء، رسالة دكتوراه، كلية الحقوق، جامعة الإسكندرية، 1999. - د. علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، الإسكندرية، 1997. - د. عمر الفاروق الحسيني، المشكلات الهامة في الجرائم المتصلة بالحاسب الآلي وأبعادها الدولية، القاهرة، 1992.

والإرادة أي علـم الجـاني بـأن البيانـات التـي يعالجها هـي بيانات شـخصية يمثل إفشـاؤها اعتـداء على الـشرف أو الاعتبـار أو حرمة الحيـاة الخاصـة مع علمـه أنه يفشي هـذه البيانات إلى شـخص غير جائـز لـه قانونًا الاطـلاع عليها، وزيادة عـلى ذلك نتيجـة إرادته إلى ارتـكاب فعل الإفشـاء أيا كانـت صورته أو وسـيلته[1].

أما الصورة الثانية: أي الخطأ فمستفادة مما أشار إليه المشرع الفرنسي من العقاب على الإفشاء إذا وقع نتيجة إهمال أو رعونة أو ترك البيانات الشخصية[2].

---

(1) د. أسامة عبد الله قايد - المسؤولية الجنائية للطبيب عن إفشاء سر المهنة - دار النهضة العربية - القاهرة - 2000 ص12.

(2) د.مأمون محمد سلامة، قانون العقوبات، القسم الخاص، ج1، دار الفكر العربي، 1982 - 1983. - د. ماجد عمار، المسؤولية القانونية الناشئة عن استخدام فيروس برامج الكمبيوتر ووسائل حمايتها، دار النهضة العربية، القاهرة، 1989. راجع في الموضوع نفسه: د. محمد حسين منصور، المسؤولية الإلكترونية، منشأة المعارف، الإسكندرية، 2006. وكذلك د. محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، دار النهضة العربية، 1984 والمادة ٤٣ من قانون المعالجة الإلكترونية والحريات الفرنسي.

الفرع الثالث

جريمة الانحراف عن الغرض أو الغاية من المعالجة الإلكترونية

مما لاشك فيه أن أشد الأخطاء التي تصيب الفرد في خصوصية معلوماته بوصفها من أهم أوجه الخصوصية المقصودة من معنى هذا الحق عند اتصاله بالحاسب الآلي هو أن المعلومات التي تجمع عن فرد من الأفراد لغرض معين ومحدد ابتداء تستخدم لدى تخزينها في الحاسب الآلي استخدامات عديدة تتجاوز الهدف الذي جمعت من أجله في الأساس[1].

فالانحراف في مجال المعالجة الإلكترونية هو الخروج عن الغرض أو الغاية الأساسية التي من أجلها تم الفعل إلى غرض أو غاية غير مقررة قانونًا ويتمثل ذلك الغرض أو الغاية بالإساءة إلى السمعة أو بالمراقبة أو بتوحيد ومحو الشخصية أو الاستغلال التجاري أو من أجل الضغط والابتزاز السياسي ونحوها لذلك فإن جميع هذه الاستخدامات غير المتوقعة[2] من أية جهة كانت يؤدي إلى إيذاء الفرد وتقليل فرص تمتعه بحقوقه على الوجه الأكمل بل تصبح قيدا على حريته فيما يريد القيام به من الأمور ومما لا جدال فيه أن نوع المعلومات التي يعطيها الإنسان عن نفسه وحجمها تختلف من جهة إلى أخرى وذلك وفقا للهدف الذي دفع هذا الفرد إلى إعطاء تلك المعلومات وعليه لكي تقوم هذه الجريمة ينبغي توافر ركنها المادي والمعنوي وفيما يلي إيجاز ذلك[3]:

(1) د. محمد عبد المحسن المقاطع - حماية الحياة الخاصة للأفراد وضماناتها في مواجهة الحاسوب الآلي - ذات السلاسل للطباعة والنشر - الكويت -)1992 ص45.

(2) د. نعيم مغبغب - مخاطر المعلوماتية والإنترنت - دار النهضة العربية - القاهرة - 1998 ص32.

(3) د. محمود نجيب حسني، شرح قانون العقوبات – القسم الخاص، دار النهضة العربية، 1994. وكذلك - المستشار معوض عبد التواب، الوسيط في شرح جرائم التخريب والإتلاف =

أولا: الركن المادي:

يتمثل بسلوك صادر عن الجاني وهو فعل الانحراف عن الغرض أو الغاية من المعالجة الإلكترونية للبيانات الشخصية، ويستوي لدى القانون أن يكون الشخص حائزا لهذه البيانات بغرض تصنيفها أو نقلها أو تسجيلها أو معالجتها تحت أي شكل كما يقتضي ليعد هذا الركن متحققا ضرورة تحديد الغاية أو الغرض من المعالجة الإلكترونية للبيانات إذ هو المناط في تحديد الانحراف أو الخروج عن الغاية أو الغرض الذي من أجله تمت المعالجة الإلكترونية للبيانات الشخصية.

والهدف من ذلك أي تحديد الغاية من المعالجة الإلكترونية هو تحقيق الرقابة لتجنب إساءة استخدام البيانات على النحو المتقدم ولكن مما يدعو للقلق في هذا الشأن هو أنه في أثناء مرحلة الرقابة قد تستغل أجهزة الحاسوب وخصوصا إمكانياتها التخزينية التي تستخدمها الأجهزة الأمنية ومنظمات ومؤسسات الخدمات المعلوماتية للتعرف على كل تحركات الأفراد وحياتهم ومعظم خصوصياتهم مما يجعل الفرد أسيرا للمعلومات التي جمعت عنه وخزنت في هذه الآلة.[1]

ثانيا: الركن المعنوي:

ويتخذ صورة القصد الجنائي العام بعنصرية العلم والإرادة أي يجب أن يعلم الجاني بأن فعله من شأنه أن يشكل انحرافا عن الغرض أو الغاية من

= والحريق، دار المطبوعات الجامعية، الإسكندرية، 1989. وراجع أيضاً د. نائلة عادل محمد فريد، جرائم الحاسب الآلي الاقتصادية، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت - لبنان، 2005.

(1) د. محمود صالح العادلي، الجرائم المعلوماتية ماهيتها - صورها، ورقة عمل مقدمة إلى ورشة العمل الإقليمية حول تطوير التشريعات في مجال مكافحة الجرائم الإلكترونية التي أُقيمت في مسقط 2 - 4 ابريل 2006 بالتعاون مع مركز التميز العربي التابع للاتحاد الدولي للاتصالات، ص37.

المعالجة للبيانات الشخصية ومع ذلك تتجه إرادته إلى تحقيق ذلك فإذا استغل شخص بيانات خاصة لآخر في الكشف عن مركزه المالي أو حالته الصحية أو في الاستدلال عليه أو في الكشف عن مصادر ثروته أو تهربه من الضرائب أو الكشف عن أية بيانات خاصة من هذا القبيل فإنه يعد مرتكبا لهذه الجريمة[1]

---

(1) د. نائلة عادل محمد فريد، جرائم الحاسب الآلي الاقتصادية، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت - لبنان، 2005 وراجع أيضاً - د. هدى حامد قشقوش، مرجع سابق ص 169.

الفرع الرابع

جريمة قرصنه البريد الإلكتروني

إن واقعة الاعتداء على البريد الإلكتروني تشكل العديد من الجرائم المبينة نصاً في قوانين العقوبات؛ وهي تتعدد بتعدد غرض الجاني(القصد الجنائي) وسلوكه الإجرامي، فهو فعل واحد إلا أن الجرائم تتعدد وتتنوع، سواء كانت لدافع إجرامي واحد أم لدوافع متعددة.

فبمجرد وقوع الاختراق تتحقق جريمة انتهاك الحرمة، فكما لا يجوز الدخول إلى المساكن والسيارات وتفتيش الحقائب، لا يجوز أيضاً الدخول إلى البريد الإلكتروني، وبما أن هذه الانتهاكات تمثل جرائم يعاقب عليها القانون؛ فإن اختراق البريد الإلكتروني يمثل جريمة يعاقب عليها القانون.

أما إذا استعمل الجاني البريد الإلكتروني وهو خاص بالغير على اعتبار أنه هو صاحبه خصوصا في مخاطباته مع الغير أو توجيه أو استقبال مراسلات عليه فهو يعتبر انتحال للشخصية، حيث إن الإيميل - كما تقدم ذكره - يرقى ليتمازج مع شخص صاحبه، إذ أن العلاقات المميزة للبريد إلكتروني عن غيره هي ذاتها التي تميز الشخص الطبيعي في العالم الإلكتروني، إذ يعرف الشخص بمسمى بريده الإلكتروني، ومن ثم يكون الجاني قد استعمل اسم الشخص صاحب البريد الإلكتروني (المجني عليه) وانتحل شخصيته في العالم الإلكتروني.

وهذه الجريمة هي ذاتها الجريمة المنصوص عليها في المادة 355 عقوبات والتي تنص علي أنه: (يعاقب بالحبس مدة لا تتجاوز سنة كل من ضلل الغير بانتحال شخصية أخرى لتحقيق منفعة لنفسه أو للغير أو لإلحاق ضرر بآخرين، أو انتحل لنفسه أو لغيره اسماً مزوراً أو صفة كاذبة أو انتحل

صفة تترتب عليها آثار قانونية، كل هذا ما لم يكن الفعل جريمة أشد ضد الثقة العامة.[1]

أما إذا اختلس الجاني أشياء أخرى أو ممتلكات موجودة فإنها إضافة إلي ما ذكر تمثل جريمة سرقة إذا ما اكتملت فيها الأركان، وفي بعض الأحيان لا تقتصر المسؤولية على الجاني بل تتعداه إلى الغير، وذلك عندما تقع الجريمة من داخل مقهى إنترنت على سبيل المثال، أو من غير صاحب الخط الخاص، عندها تكون المسؤولية مسؤولية مركبة، ليست مقتصرة على الجاني فقط.[2]

أولا:المسؤولية الجنائية:

لاشك أن السطو على الإيميل يمثل جريمة يعاقب عليها القانون، سواء في أحكام التشريعات التقليدية أم تشريعات الإنترنت، وأهيب بالمشرع إلى إصدارها فإذا ما تبين أن شخصاً ما تم ضبطه في جريمة سطو، سواء بالإجراءات المذكورة أعلاه أو بأي إثبات آخر، فإن فعله هذا يحمله المسؤولية الجنائية، التي يترتب عليها العقاب، الذي من شأنه أن يرتدع به الجاني، كما يعتبر به الغير. [3]

ثانيا: المسؤولية المدنية:

إن الجرم الجنائي يمثل خطأ، وهذا الخطأ ينشأ عنه ضرر / وبالتالي فإن المسؤولية تكون تكاملت بتوافر عناصرها (الخطأ والضرر وعلاقة السببية)، وبالتالي فإن كل خطأ سبب ضرراً للغير يلزم مرتكبه بالتعويض فيكون من حق المتضرر أن يطالب محدث الضرر بالتعويض. [4]

---

(1) عثمان سعيد المحيشي، ورقة عمل مقدمة للمنظمة العربية للتنمية الإدارية،المؤتمر الدولي الأول لقانون الإنترنت، 2005 ص 41.

(2) د. هلالي عبد اللاه أحمد، تفتيش نظم الحاسب الآلي، ط1، دار النهضة العربية، القاهرة 1997.

(3) سليمان بن مهجع العنزي: وسائل التحقيق في جرائم نظم المعلومات، رسالة ماجستير في العلوم الشرطية، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، الرياض 2003م ص 120.

(4) (W.K.Henrik) aspersen:››computer crime and other crime against

وهـذه هـي القواعـد العامـة للمسـؤولية المدنيـة، إلا أن الخصوصيـة التـي يمكـن إضافتهـا في الخطـأ المترتـب عـلى جرائـم السـطو عـلى البريـد الإلكـتروني، تكمـن في أمرين هما :

الأول: وهـو ضرورة مراعـاة خطـورة السـطو وكـذا جرائـم الإنترنـت عمومـاً في تقديـر قيمـة التعويـض، إذ أنهـا ليسـت مـن الجرائـم العاديـة ومـن ثـم فـإن الأضرار الناجمـة عنهـا عـادة تكـون بليغـة، وأرى أن يـترك تقدير ذلك لقـاضي الموضـوع.

الثـاني: يحـدث هـذا النـوع مـن الجرائـم مـن صاحـب الخـط وقـد يحـدث مـن شـخص آخـر كـما في مقاهـي الإنترنـت، فـإذا أثبـت لنـا الدليـل الرقمـي أن الجـرم وقـع مـن الخـط فـإن مـن صـدر باسـمه هـذا الرقـم ومنـح لـه ترخيـص لاسـتعماله يكـون هـو المسـؤول عـن ذلـك جنائيـاً ومدنيـاً ولـو حـدث مـن الغـير، مـا لم يثبـت أنـه قـام بتنفيـذ الإجـراءات الضبطيـة المطلوبـة منـه.

فـإذا أثبـت أنـه قـام بمسـك السـجل المطلـوب وفقـا للقانـون التجـاري إذا كان مقهـى للإنترنـت - فإنـه في هـذه الحالـة تـبرأ سـاحته، أمـا إذا تبـين العكـس فإنـه يسـأل عـن تقصـيره، ويتحمـل المسـؤولية كاملـة.

وبهـذا يكـون مـن شـأن المسـؤولية المدنيـة أن تقلـل مـن جرائـم السـطو حيـث تـردع الجـاني مـن العـود، وكذلـك الغـير.

ولحساسـية جريمـة السـطو عـلى الإيميـل وعـدم انحصارهـا فقـط في جرائـم المعلومـات فـإن شـدة خطـورة جريمـة السـطو عـلى البريـد الإلكـتروني لتعـدد أبعادهـا فتصـل إلى جريمـة انتحـال الشـخصية والابتـزاز والنصـب.

ويـرى الباحـث أنـه مـن الممكـن معالجـة هـذا النـوع مـن الجرائـم بمـا هـو موجـود في التشريعـات التقليديـة حاليـاً مثـل القانـون الجنـائي والقانـون

Information Technology In Netherland OKJ Press ‹› R.I.D.P 1993‹

التجـاري والقانـون المـدني، وذلـك لفـترة مؤقتـة بصـدور تشريـع خـاص ومـع أن المسـؤولية الجنائيـة وكذلـك المسـؤولية المدنيـة مـن شـأنهما ردع الجنـاة والتقليـل مـن غلـواء وقـوع هـذا النـوع مـن الجرائـم إلا أن صعوبـة الإثبـات قـد يـؤدي إلى عـدم كفايـة القواعـد العامـة والحاجـة إلى ضرورة إصـدار تشريـع يواكـب التطـورات المعـاصرة.

المطلب الثالث

المسؤولية الجنائية للوسيط الشبكي (مقدمي خدمة الإنترنت)

إن دخول أي فرد إلى شبكة الإنترنت يمكن أن يتم بطرق عديدة ولكنه يقتضي في جميع الأحوال اللجوء إلى متعهد الوصول ومقدم الخدمة الفنية والذي يدير الآلة المتصلة فعلاً بالإنترنت ويتيح للمستخدم الوصول إلى الشبكة فمتعهد الوصول يقدم خدمات من طبيعة فنية تتمثل في ربط المشتركين بالمواقع أو بالمستخدمين الآخرين لذا يثور التساؤل عن:

- ماهية مقدمي خدمة الإنترنت **(الفرع الأول)**.
- وما موقف بعض الفقه من مسؤولية مقدمي خدمة الإنترنت **(الفرع الثاني)**.
- وكذلك موقف بعض التشريعات من مسؤولية مقدمي خدمة الإنترنت **(الفرع الثالث)**.
- وأخيراً ما موقف بعض القضاء من مسؤولية مقدمي خدمة الإنترنت **(الفرع الرابع)**.

الفرع الأول

ماهية مقدمي خدمة الإنترنت

قد يطلق على مقدم الخدمة تسميات كثيرة منها متعهد الوصول أو متعهد الخدمة أو مزود الخدمة وقد يكون شخصاً طبيعياً أو معنوياً وأن عمله ذو طبيعة فنية فهو الذي يمكن مستخدمي الإنترنت من الوصول إلى المواقع أو البريد الإلكتروني للأشخاص الذين يريدون مخاطبتهم في أي مكان في العالم. ويتمثل دور مزود الخدمة في ربط[1] مستخدمي الإنترنت بالشبكة عن طريق عقود اشتراك تؤمن لهم الدخول إلى هذه الخدمة، وسنوضح تعريف بعض التشريعات المختلفة له على النحو التالي:

1 - قانون تنظيم الإتصالات المصري: رقم 10 لسنة 2003 (المادة 10):

عرف مقدم خدمة الإتصالات بأنه: (أي شخص طبيعي أو إعتباري يستعمل خدمات الإتصال أو يستفيد منها ويقوم بتوفير أو تشغيل الإتصالات أياً كانت الوسيلة المستعملة).

2 - قانون الكويت رقم 70 لسنة 2002:

بشأن أسس وضوابط التراخيص لمقدمي خدمة الإنترنت: قد عرف مزودي خدمة الإنترنت بأنها: "تشمل شركات الإنترنت الرئيسية والفرعية المرخصة من قبل وزارة المواصلات لتقديم خدمات الإنترنت للمشتركين بما في ذلك المشتركين من مقدمي خدمة الإنترنت".

---

(1) د/ محمد حسين منصور، المسؤولية الإلكترونية، الناشر دار الجامعة الجديدة، الإسكندرية 2003، ص 209.

كما عرف مقدمي خدمة الإنترنت بأنه: "يشمل مقاهي الإنترنت "Cyber café"" ومراكز التسلية ومحلات ومراكز خدمات الكمبيوتر وأية هيئات أو جهات أو مراكز عامة أو خاصة تقدم خدمات الإنترنت بجميع أنواعها سواء كان ذلك بمقابل أم بدون مقابل[1].

(1) د/ عبد الفتاح كيلاني، المسئولية المدنية الناشئة عن المعاملات الإلكترونية عبر الإنترنت (رسالة دكتوراه) الناشر دار الجامعة الجديدة، الإسكندرية 2011، ص 189.

الفرع الثاني

موقف بعض الفقه من مسؤوليات مقدم خدمة الإنترنت

تعدد طرق الوصول إلى الإنترنت سواء عن طريق IDSL, ISDN, Dial UP, Leased Line، إلا أنه في كل الأحوال يجب وجود مقدم خدمة، ولقد أثارت مسألة مقدم الخدمة باعتباره فاعل أصلي في الجريمة الكثير من الجدل رأى يرى: مسائلته تأسيساً على أسس المسئولية التوجيهية فإنه يتعين على مقدم الخدمة منع نشر محتوى صفحات الشبكة المتعارضة مع القوانين والنظم واللوائح أو المصلحة العامة[1].

وأن مسئولية مقدم هذه الخدمة مسؤولية تعاقدية وذلك في حالة عدم تنفيذ التزامه بتمكين العميل من الدخول للشبكة ولكن لا يعد مسؤولاً عن محتوى المعلومة وذلك لأنه لا يملك الوسائل الفنية التي تمكنه من رقابة صحة هذه المعلومات ومشروعيتها وقد يضع مقدم الخدمة شروطاً تعفيه من المسؤولية أو تحد منها ومن أمثلة الشروط المحددة للمسئولية الإتفاق على حد أقصى للتعويض وفي جميع الأحوال فإنه يلزم في حالة عدم تنفيذ العقد برد قيمة إشتراك الخدمة.

وتقوم مسؤولية مقدم خدمة الإنترنت بالإضافة إلى القواعد العامة للمسؤولية عند وقوع خطأ في إبلاغ الرسالة الإلكترونية إلى المرسل إليه ناتج عن سبب راجع إليه أو أحد العاملين لديه.

كما تقوم مسؤوليته إذا أنتهك سرية المراسلات والمكاتبات والإتصالات الإلكترونية ما لم يكن تدخله تبرره الضرورة الفنية لتشغيل الشبكة وليس[2]

---

(1) د/ متولى عبد المؤمن، الجريمة عبر الإنترنت «منتدى جامعة المنصورة على الإنترنت 2008» بحث منشور على الموقع http://www.f-law.net/needex.php

(2) د/ خالد ممدوح إبراهيم، حماية المستهلك في المعاملات الإلكترونية، دراسة مقارنة، الدار الجامعية، الإسكندرية، 2007، ص 60.

لسبب آخر وفي حالة تعسفه في معالجة البيانات المعلوماتية الأسمية يمكن أن يسأل جنائياً بالإضافة إلى مسؤوليته المدنية لو سبب معالجته الخاطئة ضرر للغير[1].

رأى أخر: وهو الغالب يرى أن مسؤولية مزود الخدمة تتوقف على نوع الخدمة التى يؤديها، فإذا قام بدور الناقل الذي يربط بين كمبيوتر العميل الشخصي والخادم فهو غير مسؤول عن عدم مشروعية الإعلانات التى تبث عبر الموقع. أما إذا تعدى دوره هذا الدور البسيط وقام بوظيفة متعهد الإيواء الذي يسمح لشركة الإعلانات أو مستغل الموقع من نشر إعلانه هنا يمكن مسائلته مدنياً عن الأضرار التي يسببها للغير نتيجة الإعلانات غير المشروعة، فهذا الدور يمكنه من الإطلاع على محتوى الإعلان قبل نشره ومن ثم يكون[2] مسؤولاً عن المحتوى غير المشروع للإعلان.

رأى أخر يرى: أن دور مزود الخدمة عبر الشبكة يقتصر على ربط المستخدم بالموقع الذي يريده فهو مجرد دور فني خالص لا يتضمن أية رقابة على مضمون أو[3] محتوى الموقع الذي يختاره المستخدم بمحض إرادته، ولتوضيح علة عدم مسؤوليته يشبه البعض عمل مزود الخدمة بشخص نصح أو أشار على المستخدم الذي يشترى الصحيفة التي بها إعلان كاذب أو المقارن أو يشاهد قناة التيلفزيون التي تبث هذا الإعلان ذو المحتوى غير المشروع. وهو ذات اتجاه الفقه والقضاء الإيطاليين اللذان يذهبان إلى عدم مسؤولية مزود الخدمة لأنه لا يقوم بتوريد المعلومات ولكنه يؤمن خدمة الوصول إليها فقط.

وأرى: أن مورد المضمون غير المشروع ليس هو المسؤول وحده فهناك

---

(1) د/ أحمد حسام طه، الجرائم الناشئة عن إستخدام الحاسب الآلي، رسالة دكتوراه، كلية الحقوق، جامعة طنطا 20000، ص 81.

(2) د/ شريف محمد غنام، التنظيم القانوني للإعلانات التجارية عبر شبكة الإنترنت، دار الجامعة الجديدة، الإسكندرية، 2008، ص 149.

(3) د/ محمد حسين منصور، المرجع السابق، ص 212.

أكثر من شخص يتدخل في عملية نقل المعلومات ويمكن بالتالي دخوله في نطاق المساءلة ويشمل ذلك متعهدي الوصول والإيواء وكل من يسهل الإطلاع على المضمون غير المشروع بأي وسيلة مثل: تقديم الموتور الباحث عن الخدمة، أو بخلق إتصال مباشر بالموقع أو تقديم البرامج المقوية للربط المسهلة لتبادل مضمون بين مستخدمي الشبكة. وأنه يتعين إقامة المسؤولية لكل شخص على ضوء الدور القائم به ودرجة تدخله في تقديم الخدمة وعلى حسب ظروف كل واقعة على حده وذلك لما لديهم من التقنية والبرامج التي تكشف لهم المحتوى غير المشروع قبل بثه وتحقق للمضرور التمسك بالمسؤولية التضامنية عند الرجوع عليهم بالتعويض عن الضرر الذي أصابه.

الفرع الثالث

موقف بعض التشريعات الخاصة

من المسؤولية القانونية لمقدمي خدمة الإنترنت

إن مسؤولية مقدمي خدمة الإنترنت قد تعرضت لها العديد من التشريعات المختلفة في الدول الأجنبية والعربية.

وسنوضح بعضاً منها على النحو التالي:

أولاً: التوجيه الأوربي الخاص بالتجارة الإلكترونية:

الصادر في 17 يونيو عام 2000 الذي تضمن في المبحث الرابع (المواد من 12: 15) المنظمة لمسؤولية المؤدين المهنيين وقد أقرت نصوص هذا التوجيه عدم إلتزام الوسطاء الفنيين برقابة مشروعية المعلومات والإعلانات التي تبث عبر الموقع وإنما فرضت عليهم أن يتصرفوا بشكل مناسب لمنع الوصول إلى هذا المحتوى غير المشروع. و(المادة 12/1) من ذات التوجيه أعفت مزود خدمة الإنترنت من المسؤولية عن الأعمال غير المشروعة التي يتضمنها الموقع إذا توافرت الشروط الآتية:

1 - ألا يكون مصدر الضرر.

2 - ألا يكون قد اختار المرسل إليه الذي ينقل إليه المعلومات.

3 - ألا يختار المعلومات التي يقوم بنقلها أو يعدل فيها.

وتنص (الفقرة الثانية) من المادة ذاتها على أن مزود الخدمة يتضمن تخزين مؤقت للمعلومات التي يقوم بنقلها بيد أن هذا التخزين المؤقت لا يجعله مسؤولاً ولا يجعل عمله يرقى إلى عمل متعهد الإيواء. ومن ثم لا يسأل مساءلته.

وتجيز الفقرة الثالثة من هذا التوجيه للدول الأعضاء أن تنص في قوانينها الداخلية على التزام مزود الخدمة بأن يوقف الخدمة ويستبعد المحتوى غير المشروع للموقع[1].

ثانياً: موقف بعض القوانين الأجنبية من مسؤولية مقدمي خدمة الإنترنت:

1 - التشريع الفرنسي:

(أ) القانون الفرنسي الصادر في أول أغسطس 2000 معدلاً بعض أحكام القانون رقم 30 سبتمبر سنة 1986 المتعلق بالإتصالات السمعية والبصرية:

والذي حاول أن يزيد من حالات عدم المسؤولية سواء كانت المدنية أو الجنائية عن المعلومات التي يتم بثها عبر شبكة الإنترنت.

فقد كانت (المادة 14) من المشروع تنص على: أن الأشخاص الطبيعيين أو المعنويين الذين يتعهدون بشكل مجاني أو بمقابل، بالتخزين المباشر والمستمر من أجل وضع المعلومات تحت تصرف الجمهور بكتابات أو رسوم أو صور أو رسائل يمكن إستقبالها لا يسألون جنائياً أو مدنياً عن محتوى هذه الخدمات.

وأنه يمكن مساءلة مقدمي خدمة الإيواء عن عدم إتخاذ الإحتياطات المناسبة في حالة تحذيرهم بعدم مشروعية المضمون[2].

وقد حدد القانون المسؤولية في حالتين:

الأولى: إذا تم اللجؤ إلى القضاء ولم يقم القائم بالتخزين أو متعهد الإيواء مع ذلك بإتخاذ اللازم نحو منع وصول هذا المضمون إلى الجمهور.

---

(1) د/ محمد عبد الظاهر حسين، المسئولية القانونية في مجال شبكات الإنترنت، دار النهضة العربية، القاهرة، ص1000، 2003/2004.

(2) فيصل محمد عبد العزيز، الحماية القانونية لعقود التجارة الإلكترونية، الناشر، دار النهضة العربية، القاهرة، ص 155، 2008.

الثانية: إذا أخطره الغير بأن المحتويات التي يتولى تخزينها غير مشروعة وتسبب (15) له أضرار إلا أنه لم يقم بإتخاذ الإجراءات اللازمة لمنع بثها ونشرها.

وعلى ذلك تكون القاعدة العامة هي عدم مسؤولية الأشخاص القائمين على تخزين المعلومات أو الممارسين للإيواء عن هذه المعلومات لا جنائياً ولا مدنياً إلا إذا تم إلزامهم قضائياً برقابة مضمون ومحتوى هذه المعلومات ففي هذا الفرض تقوم مسؤوليتهم عن الأضرار التى تسببها هذه المعلومات.

(ب) القانون الفرنسي الصادر في 21 يونيه 2004: الخاص بالثقة في الإقتصاد الرقمي والذي يعد أحدث القوانين الأوربية في هذا المجال:

وقد خصص هذا القانون (المواد من 5: 9) في الفصل الثاني منه لتنظيم عمل المؤدين الفنيين Les Prestataires technique وفقاً (للمادة 6/1) للأشخاص الذين يقتصر عملهم على تقديم خدمة الإتصال عبر الإنترنت (يقصد مزود الخدمة) يجب أن يخطروا المشتركين في الخدمة عن وجود وسائل تقنية تسمح بغلق الخدمة أو توقع جزاءات عليهم إذا توافرت شروط توقيعها وأكدت الفقرة السابعة من هذه المادة أن مزودي الخدمة ليس عليهم الإلتزام بالإشراف والرقابة على مضمون البيانات التي يقومون بنقلها كما أنهم غير ملتزمين بالبحث عن الوقائع التي تشير إلى الأنشطة غير المشروعة[1].

وفي 15 مايو 2009 يقر مجلس الشيوخ الفرنسي سن مشروع قانون مسؤولية مقدمي خدمات الإنترنت للقرصنة على الإنترنت نهج إستجابة تخرج وسائل (مقدمي خدمات الإنترنت) الرد على انتهاكات حقوق الملكية الفكرية المعروفة، والتي تتكرر على شبكاتهم من خلال إرسال تحذيرات لهؤلاء العملاء في المقام الأول، وقطع خدماتهم في (17) نهاية المطاف، إذا ما فشلت في الإستجابة للتحذيرات المتكررة وغيرها من التدابير.

---

(1) د/ محمد عبد الظاهر حسين، المرجع السابق، المسؤولية القانونية في مجال شبكات الإنترنت ص 101 وما بعدها.

2 - التشريع الأمريكي:

في أمريكا تتضمن نصوص القانون الأمريكي لحماية حق المؤلف عبر شبكة الإنترنت الذي صدر في 28 أكتوبر 1998 ودخل حيز النفاذ في 1 أكتوبر 2000 وقد نص في (المادة 2/5) منه التي تبرأ مزود الخدمة الذي يقتصر دوره على مجرد نقل بسيط للمعلومات من الغير إلى الموقع من أية مسؤولية ناتجة عن (18) المحتوى غير المشروع لهذه المعلومات.

3 - التشريع البريطاني:

قد أصدرت بريطانيا تشريعها الخاص بتنظيمات التجارة الإلكترونية قد دخل حيز التنفيذ في 23 أكتوبر 2002 ففي هذا القانون نقلت أحكام التوجيه الأوربي في (المواد 12، 13، 14) المتعلقة بمسؤولية مزود الخدمة ومتعهد الإيواء سالفة الذكر التي نحيل إليها.

ثالثاً: موقف بعض القوانين العربية من مسؤولية مقدمي خدمات الإنترنت:

1 - التشريع المصري:

تضمن قانون حماية المستهلك رقم 67 لسنة 2006 في (المادة 9) على: (التزام مقدم الخدمة بإعادة مقابلها أو مقابل ما يجبر النقص فيها أو إعادة تقديمها إلى المستهلك وذلك في حالة وجود عيب أو نقص بها).

2 - التشريع الكويتي:

كما حدد القانون الكويتي رقم 70 لعام 2002 سالف الذكر، الالتزامات المفروضة على عاتق مقدمي خدمة الإنترنت في (المادة الثالثة) والتي من أهمها الالتزام بتركيب وتشغيل أنظمة الرقابة الكفيلة بمنع المواد والمواقع الإباحية أو المخالفة للدين والعادات والأمن وبالوسائل المختلفة مثل صفحات الإنترنت أو برامج المحادثة أو البريد الإلكتروني أو سواها، مع التحديث المستمر لمواكبة التغيير في المواقع والعناوين الجديدة وتكون

هـذه الأنظمـة الرقابيـة إضافيـة ومكملـة للأنظمة الرقابيـة لدى مزودي خدمـة الإنترنت، الالتـزام بتسـجيل البيانـات الأساسـية لمستخدمي خدمـات الإنترنـت، ومنـع تقديـم أي مـن خدمـات الإنترنـت لمـن هـم دون سـن الثامنـة عـشرة. وأرى: أن هذا التشريـع موفق لتمشـيه مـع أحـكام الشريعـة الإسـلامية والتطـور التكنولوجـي الحديث.

3 - التشريـع البحريني:

الصـادر في 14 سـبتمبر 2002 بشـأن المعامـلات الإلكترونيـة نظم ذلـك في (المادتين 18، 19) منـه عـلى مسـؤولية وسـطاء الشـبكات عـلى أنـه لا تقـوم المسـؤولية المدنيـة أو الجنائيـة تجـاه مقـدم خدمـة الإنترنـت بشـأن أيـة مـادة خاصـة بالغـير وتكـون في شـكل سـجلات إلكترونيـة وكان دوره مقصـور عـلى مجـرد إمكانيـة اسـتخدام الشـبكة دون أن يكـون هـو المنشـئ لتلـك المـادة وهـذا إن كانـت مسـؤوليته قائمـة عـلى حالتـين:

1 - علـم أو نـشر أو إصـدار أو توزيـع هـذه المـواد بشـكل سـجلات إلكترونيـة أو أيـة بيانـات تتضمنهـا هـذه المـواد.

2 - انتهـاك أيـة حقـوق قائمـة بخصـوص هـذه المـواد أو مـا يتعلـق بهـا وذلـك شريطـة عـدم وجـود معرفـة فعليـة أو علـم لـدى وسـيط الشـبكات بـأن المـواد في هـذه السـجلات مـن شـأنها إيجـاد مسـؤولية مدنيـة أو جنائيـة[1].

(1) د/ عبد الفتاح محمود الكيلاني، الرسالة السابقة ص 195.

الفرع الرابع

موقف القضاء من مسؤولية مزود خدمة الإنترنت

اختلفت الاتجاهات القضائية بشأن مسؤولية مزود الخدمة فتارة يقرون بمسؤوليتهم وتارة أخرى يبرؤون ساحتهم، ونوضح موقف بعض القضاء المختلف. على النحو التالي:

أولاً: القضاء الفرنسي:

(أ) ففي حكم صادر من المحكمة الإبتدائية بباريس في أكتوبر 1999 في قضية EDV:

انتهت المحكمة إلى أن مزود الخدمة عبر شبكة الإنترنت ليس مسؤولاً عن طبيعة ومشروعية المعلومات التي ينقلها إلى المستخدمين وتتمثل وقائع القضية في أن شركة EDV قامت بنشر مقالة بعنوان: "المشروعات الصغيرة كيف تختار نظامها المالي" دون موافقة من مؤلف هذه المقالة. وبغرض نشر هذه المقالة على موقعها استعانت رفع للخدمة كمزودتين ".UUNet France et UUNet Technologie inc" بشركتي المؤلف دعواه ضد الشركة صاحبة الموقع والشركتين مزودتي الخدمة لسحب المقالة والتعويض عن الأضرار التي أصابته من جراء النشر عبر الإنترنت. أكدت المحكمة عدم مسؤولية مزودي الخدمة بحجة أن: (عملها قد أقتصر على نقل المعلومات من الموقع إلى المستخدم، ولذا فإن الشركتين مزودتا الخدمة غير مسؤولتين عن طبيعة ومشروعية البيانات التي تم بثها على هذا الموقع[1].

(1) وقائع القضية واردة على الموقع:

http://www.Afa-France.com/html1/action/jugement2.html

(ب) وفي قضية اتحاد الطلاب اليهود التي رفعها ضد شركة Yahoo بإعتبارها مزود الخدمة:

انتهت المحكمة إلى أنها تعد مسؤولة عن عدم مشروعية الإعلانات والأعمال التي تمت عبر موقعها Yahoo.com المخصص لبيع أشياء تتعلق بالنازية بالمزاد العلني، ولكن مسؤوليتها تنشأ فقط منذ العلم بالمحتوى غير المشروع للموقع.

ويذهب القضاء الفرنسي أن مجرد قيام مستخدم الشبكة ببث رسالة غير مشروعة لا يكفي لقيام مسؤولية مقدم خدمة الإنترنت وذلك أخذاً في الاعتبار العدد اللانهائي للمشتركين وحجم الرسائل الضخم المتداول يومياً[1].

ثانياً: موقف القضاء الأمريكي:

وهو ما أيدته إحدى المحاكم الأمريكية حيث قضت بعدم مسؤولية مزود خدمة الإنترنت عما يرتكبه الآخرين من جرائم وفق قانون الأخلاق والإتصالات الأمريكي الصادر سنة 1996، قضت أحد المحاكم الأمريكية بأن وضع كاميرا الإنترنت في غرفة تغيير ملابس الرياضيين في الجامعة لمراقبتهم دون علمهم يعفي مزود خدمة الإنترنت من المسؤولية حيث إن دوره يقتصر على خدمة الإتصال فقط[2].

ثالثاً: القضاء المصري:

أصدرت محكمة القضاء الإداري المصرية حكم يدعم حرية الإنترنت

---

(1) أقرت المحكمة حجة اتحاد الطلاب اليهود بان شركة Yahoo هي التي تمكن الجمهور من الوصول إلى هذا الموقع الذي يروج أشياء تتعلق بالنازية بل ذهبت بعض الأحكام إلى أبعد من ذلك عندما استندت إلى أحكام قانون العقوبات الفرنسي خاصة (المادة 2/323) التي تعاقب كل من قام عمداً بإعاقة عمل جهاز من أجهزة المعلوماتية وقائع.

(2) د/ عمر محمد بن يونس، أشهر المبادئ المتعلقة بالإنترنت لدى القضاء الأمريكي، بدون ناشر، 2004، ص 83.

الصادر بجلسة 29 ديسمبر 2007 في الدعوى رقم 15575 لسنة 61 فتتلخص وقائع هذه الدعوى في طلب المدعي الحكم بصفة مستعجلة بوقف تنفيذ وإلغاء القرار الإداري السلبي الصادر من وزير الاتصالات بصفته بالامتناع عن حجب المواقع الإلكترونية الإرهابية المشار إليها في صحيفة الدعوى وإغلاقها أينما وجدت على شبكة الإنترنت.

ومن حيث أنه سبق لهذه المحكمة بهيئة مغايرة أن انتهت إلى أن التشريعات المصرية لم تحدد المجالات التي تستدعي حجب المواقع الإلكترونية غير أن هذا الفراغ التشريعي لا يخل بحق الأجهزة الحكومية من إلزام مزودي الخدمة بالحجب حينما يكون هناك مساس بالأمن القومي أو المصالح العليا للدولة وذلك بما لتلك الأجهزة من سلطة في مجال الضبط الإداري لحماية النظام العام وانتهت المحكمة برفض الدعوى تأسيساً على ما تقدم[1].

(1) القضية متوافرة على الرابط التالي:

http://www.adaweya.net/showthread.php?t39298

الخاتمة

إن مبدأ حماية البيانات الشخصية يعد منبثقا من مبدأ الخصوصية وتعد خصوصية البيانات الشخصية أحدث أنواع الخصوصية وبما أن الخصوصية تحمي الحق في التستر والاستمتاع بالمساحة الشخصية وكذلك تكفل حماية البيانات الحق في حماية الشخص لبياناته ومعلوماته الشخصية التي يفصح عنها طواعية أو التي يمكن الوصول إليها بشكل.

وقد ارتبط مفهوم الخصوصية حديثاً بمفهوم خصوصية البيانات الشخصية والبيانات الشخصية هي تلك البيانات التي يمكن خلالها تعريف الشخص تعريفاً محدداً أو الاستدلال عليه.

واتسع مفهوم البيانات الشخصية حتى شمل أيضاً آراء الشخص ومعتقداته وتوجهاته السياسية والعقائدية.

وقد فرض التطور التكنولوجي في عالم الاتصالات وضع مفهوم أشمل لتلك البيانات فقد يعبر الشخص عن حالته المزاجية أو رأيه السياسي عبر مواقع التواصل الاجتماعي ويعد ذلك بياناً شخصياً.

ولا تفقد البيانات الشخصية الحماية بمجرد علانيتها أو الإفصاح الطوعي عنها حيث إن الاستيلاء على البيانات أو معالجتها بدون وجه حق حتى وإن كانت معلنة يمثل اختراقا لحماية البيانات الشخصية.

وقد زادت مخاطر التعدي على البيانات الشخصية بثورة الاتصالات والإنترنت مما أدى إلى المحاولات الدولية لحماية البيانات الشخصية عبر الإنترنت.

وبالنسبة لتصنيف البيانات الشخصية فإنها يمكن أن تصنف من حيث الناحية الاجتماعية والصحية والخصائص البيومترية والتعليمية وكذلك الوظيفية والمهنية.

و لقد ظهر ما يسمى بـ "الخصوصية الرقمية" هي وصف لحماية البيانات الشخصية للفرد، والتي يتم نشرها وتداولها من خلال وسائط رقمية. وتتمثل البيانات الشخصية في البريد الإلكتروني، والحسابات البنكية، والصور الشخصية، ومعلومات عن العمل والمسكن وكل البيانات التي نستخدمها في تفاعلنا على الإنترنت أثناء استخدامنا للحاسب الآلي أو التليفون المحمول أو أي من وسائل الاتصال الرقمي بالشبكة العنكبوتية.

وقد أدى إتاحة شبكة الإنترنت للجمهور منذ عام 1991 في إحداث نقلة سريعة في مجال تكنولوجيا المعلومات بعد أن كان مُقتصراً على الأبحاث الأكاديمية والعسكرية فقط. كما تَبِع ذلك تطور البرمجيات التي سهلت استخدام الإنترنت فتضاعف مستخدمي الإنترنت من 360 مليون نسمة عام 2000 إلى ما يقارب 2.7 مليار نسمة في عام 2013.

ومع تزايد التقنيات الحديثة وتطورها المستمر زادت المخاطر على الخصوصية، فكثيرة هي الابتكارات التكنولوجية التي أصبحت اليوم تقيد الفرد في تنقلاته، وترصد أعماله وحركاته، وتجمع البيانات الشخصية حوله وتخزنها وتعالجها بواسطة الوسائل المعلوماتية كتقنيات المراقبة بالفيديو، ورقابة البريد والاتصالات وقواعد البيانات وغيرها. وهي جميعها تؤلف تهديدا مباشرا وجديدا على الحياة الخاصة وللحريات الفردية خاصة بصورتها المستحدثة والمتمثلة في بنوك المعلومات.

لا سيما إذا استغلت المعلومات والبيانات المجمعة لغايات وأغراض مختلفة بدون رضا أصحابها الذين قد لا يكونون أصلا على علم بوجودها.

وتوَسَع استخدام الإنترنت من الأغراض البحثية إلى تقديم خدمات مختلفة للجمهور مثل البريد الإلكتروني والمراسلة الفورية والشراء والبيع عبر الإنترنت. فصار تفاعل الأفراد مع الشبكة أكثر اقتراباً وتأثيراً في حياتهم اليومية. جميعنا يستخدم البريد الإلكتروني وكذلك مواقع التواصل الاجتماعي بصفة يومية ومنا من يقوم بعمليات الشراء بين الحين والآخر؛ وبالتالي أصبح الإنترنت أكثر تماساً مع خصوصيتنا.

ونظرا لتزايد تفاعل الأفراد مع العالم الرقمي أصبحت الخصوصية مهددة وصارت البيانات الشخصية مادة يتم استخدامها إما تجارياً في تنفيذ دعاية تسويقية، أو مراقبتها من قِبل جهات حكومية، أو تعرضها للسرقة واستغلالها في أغراض تضر بأصحابها.

وكوْن الحفاظ على الخصوصية الرقمية قضية حديثة العهد فإن التعامل مع التجاوزات التي تؤثر فيها من قِبل الحكومات، أو أية أطراف أخرى تحتاج إلى العديد من التوجيهات عن كيفية حمايتها من خلال تحديث الأطر القانونية ذات الصلة.

ولا نزاع اليوم في أن الخصوصية تعد من الحقوق الدستورية الأساسية الملازمة للشخص الطبيعي بصفته الإنسانية كأصل عام، فهي تعد أساس بنيان كل مجتمع سليم، وهو يعتبر من الحقوق السابقة على وجود الدولة ذاتها.

لذا تحرص المجتمعات خاصة الديمقراطية منها على كفالة هذا الحق، وتعتبره حقا مستقلا قائما بذاته، ولا تكتفي بسن القوانين لحمايته بل تسعى إلى ترسيخه في الأذهان، وذلك بغرس القيم النبيلة التي تلعب دورا كبيرا وفعالا في منع المتطفلين من التدخل في خصوصيات الآخرين وكشف أسرارهم.

ولقد حظي هذا الحق باهتمام كبير سواء من جانب الهيئات والمنظمات الدولية أو من جانب الدساتير والنظم القانونية.

ويمثل حماية خصوصية البيانات في البيئة الرقمية حماية المعلومات من حيث توافرها وإضفاء الثقة فيها وتأكيد سلامتها. ويعبر توافر Availability المعلومات علي خاصية من خصائص نظم المعلومات الممكن الوصول إليها واستخدامها علي أساس فوري في إطار نمط محدد ومطلوب، كما يصبح في الإمكان الوصول إلي النظام عندما يطلب بطريقة معتمدة ووفقا لمواصفات ملائمة لهذا للنظام؛ وتعتبر السرية Confidentiality خاصية ترتبط بعدم تغيير البيانات والمعلومات أو فقدها أو إهدارها وإتاحتها فقط لأشخاص وكيانات معتمدة ومصرح لها فقط باستخدامها، وتتضمن العمليات التي تستخدم أساليب التشفير والحجب لمحتويات البيانات والمعلومات أو السماح بها في أوقات وفي طرق معتمدة.

أما السلامة Integrity فهي خاصية البيانات والمعلومات الدقيقة والكاملة التي تحفظ بدرجة كبيرة من الدقة والاكتمال، وتتنوع الأولوية والأهمية النسبية لتوافر المعلومات وسريتها وسلامتها طبقا لنظام المعلومات المتاح.

ويتضح أن إدارة أمن المعلومات والحفاظ على خصوصية البيانات هي قضية أخلاقية في المقام الأول، حيث يتوصل فيها إلي توازن بين قيمة المعلومات للمنظمة من جهة وتكلفة الأفراد والمقاييس الإدارية والتكنولوجية من جهة أخرى. وتضع مقاييس الأمن الحاجة في التوصل إلي أقل تكلفة من المخاطر أو الأضرار التي قد تسبب فقد سرية المعلومات وتحد من سلامتها وتوافرها.

وكذلك فإن نقص التدريب والتوعية الملائمة عن خصوصية البيانات وأمن المعلومات وأهميته تسهم في الجهل باستخدام نظم المعلومات المناسبة.

وبدون تنظيم دورات تدريب ملائمة، قد يجهل كثير من العاملين

والمستخدمين بأعراض الأضرار النابعة من سوء استخدام نظم المعلومات، كما قد لا يستخدمون أي مقاييس أمن حتى البدائية منها، مما قد يؤدي إلي مزاولات تعود بالإساءة لأمن المعلومات. ويقدم اختيار كلمة المرور **Password** الذي يمثل نشاط المستخدم في كل أنحاء العالم بل يمثل النشاط الرئيس لأي نظام معلومات مثالا واضحا لأمن المعلومات.

فعلي الرغم من أن كلمات المرور تطبق عادة علي رقابة الوصول إلي معظم نظم المعلومات، فلا يزال عدد قليل جدا من المستخدمين يعلم بأهمية الحاجة لأمن كلمة المرور بالطريقة التي تتمثل في تحديد أو إنشاء كلمة المرور ومن العواقب التي تتمثل في سوء استخدام النظام.

ولم تناقش التشريعات العربية سوى حماية البرمجيات والملكية الفكرية لمثل هذه الابتكارات وذلك اعتقادا منا لمواكبة متطلبات السوق العالمية بالإضافة إلى وجود المنظمة العالمية للملكية الفكرية (الوايبو).

وقد تطورت قوانين حماية الخصوصية المعلوماتية بشكل كبير في جميع دول العالم فوجدنا أن الولايات المتحدة الأمريكية لديها مجموعة من القوانين المتسلسلة في هذا الشأن ونجد أن المملكة المتحدة اتخذت من التوجيه الأوروبي لحماية البيانات الشخصية نموذجاً وقد احتذت به وأصدرت القانون الخاص بها في حماية البيانات الشخصية.

وبالمقارنة بين هذه القوانين والإرشادات والتوجيهات الصادرة من مختلف الهيئات الدولية نجد أن هناك مبادئ عامة في مجال حماية البيانات الشخصية عبر الإنترنت وهي كما يلي:

- أن يتم معالجة البيانات الشخصية بشكل عادل وقانوني.
- أن يتم الحصول على البيانات الشخصية فقط لغرض أو أكثر من الأغراض المحددة والقانونية كما أنه لن يتم معالجتها بأي شكل لا يتوافق مع ذاك الغرض أو تلك الأغراض.

- البيانات الشخصية تكون مناسبة ومعنية وغير مسهبة فيما يتعلق بالغرض أو الأغراض التي يتم معالجتها لأجلها.

- يجب أن تكون البيانات الشخصية دقيقة وأن يتم تحديثها متى تطلب الأمر ذلك.

- لا يتم الاحتفاظ بالبيانات الشخصية التي يتم معالجتها لأي غرض من الأغراض لما يزيد عن المدة الضرورية اللازمة لذاك الغرض أو تلك الأغراض.

- فيما يخص حقوق الأفراد على سبيل المثال، يتم معالجة البيانات وفقا لحقوق الأفراد أصحاب البيانات ويتم اتخاذ الإجراءات الفنية والتنظيمية المناسبة ضد المعالجة غير المرخص بها أو غير القانونية للبيانات الشخصية وضد الفقد أو التلف العفوي أو الضرر الواقع على البيانات الشخصية.

وبالرغم من هذه المبادئ والقوانين فإن البيانات الشخصية المتداولة عبر الإنترنت لا تتمتع بالحماية اللازمة وذلك حيث إن التطور في عالم الاتصالات لا يستطيع معه القانون التواؤم فالاطراد المتنامي في هذا المجال لا يجعل خبراء المجال نفسه في حالة علم كامل ودراية بتلك المستجدات المتلاحقة ولكن هناك واجب على المشرعين وخاصة المشرع العربي في هذا المجال حيث عليه بالبحث وسن القوانين لمواجهة الانتهاكات التي تلاحق البيانات الشخصية عبر الإنترنت.

بالإضافة إلى أن هناك جانب آخر يجب العمل عليه وهو زيادة التوعية بأهمية الحفاظ على البيانات الشخصية وعدم الإفصاح عنها إلا إلى ضرورة معينة، فنجد أن كثيرا من مستخدمي الشبكة العنكبوتية يتعاملون مع الشبكة على أساس يومي بدون ثمة دراية عن إجراءات الحماية فالآلاف بل الملايين يستخدمون يوميا مواقع التواصل الاجتماعي بداية من إنشاء حسابات عبر تلك المواقع أو نشر صور وأخبار ومعلومات وتحديث بياناتهم بشكل دوري.

ولا يقوم الكثير من مستخدمي تلك الشبكة بقراءة سياسات الخصوصية التي تظهرها تلك المواقع معلنة فيها إلى أي مدى سوف تقوم بمعالجة البيانات ويعد هذا تحصينا قانونيا لمثل هذه المواقع حتى إن قامت الأخيرة بمعالجة البيانات تنتفي مسؤوليتها القانونية

وهنا يظل المستخدم رغما عن تقصيره في بعض الأحيان هو المضرور الرئيس من الفراغ التشريعي والقصور في مجال حماية البيانات الشخصية إذ يقوم المستخدم بالاستفادة بما تقدمه الشبكة الإلكترونية من خدمات في حياته العملية والاجتماعية دون دراية أنه يتخلى عن حقه في الخصوصية لمعلوماته.

إضافة إلى أن الدخول على شبكة الإنترنت هذه الأيام لا يتطلب أسلاكا ولا حتى أجهزة كمبيوتر فيكفي فقط أن تمتلك هاتفا ذكياً له القدرة على الدخول على شبكة الإنترنت ومن ثم زادت البرامج والتطبيقات التي تمتص البيانات الشخصية للأفراد وكلما زاد ارتباط الشخص بالتكنولوجيا كلما قلت فرص حماية بياناته الشخصية وهناك من البرامج التي تعلن هذا صريحاً في سياساتها للخصوصية والتي غالبا ما يوافق عليها مستخدم البرامج دون قراءه، إن لها الحق في الاطلاع واستخدام البيانات المسجلة على حسابه أو على الجهاز الذي يشغل البرنامج من خلاله الأمر الذي مكن برنامج True caller من التسلل إلى قوائم الأسماء والبيانات على تليفونات مشغلي البرنامج وتكوين قاعدة بيانات عملاقة تمكنه بعد ذلك من توفير خدمة معرفه اسم المتصل دون تسجيل اسمه على سجل الهاتف.

إن حماية البيانات الشخصية شأنها شأن أي مستحدث يجب أن تلاحق بالتشريع والحماية لكن الأمر هنا يختلف لتعلق هذا المستحدث بشيء سريع النمو والاطراد.

وتبقى المشكلة ليس فقط في وضع تشريعات وسن قوانين ولكن العائق هنا وأمام لا مركزية شبكة الإنترنت فتثور مسائل عدة بشأن القواعد الإجرائية لضبط الجرم وتوقيع العقاب على المستولي فلهذا وتزامننا مع وضع

التشريعات وجب تحديث البيئة المعنية بتطبيق مثل هذا النوع من القوانين بعد سنها، إذ أنه مع وجود قوانين دون معرفة كيفية آليات تنفيذ هذه القوانين تعد تلك غير ذات جدوى وجهدا مبذولا لن نجد منه مردوده المرجو.

وتستند التشريعات التي تدافع عن الخصوصية على تعريفها كقيمة مهمة لدي أفراد المجتمع. ونظرا لحداثة موضوع الخصوصية الرقمية تختلف الأطر التشريعية من دولة لأخرى طبقا للمستجدات التي مرت بها كل دولة، وفلسفتها التشريعية، وكيفية تطبيقها للقوانين والتحولات التي يمر بها المجتمع ومقدرة كل دولة على تبني تعديل لقوانينها بناء على قضايا جديدة تكون خارج إطارها التشريعي.

تهتم قوانين الخصوصية بحماية وسائط نقل المعلومات إما عبر الإنترنت أو الهواتف أو حتى البريد، كما تتضمن الحفاظ على سرية المعلومات الخاصة للأفراد الموجودة في سجلاتهم مثل المعلومات المالية أو الصحية. كما يجب أن تضمن بياناتهم الخاصة التي يتم تداولها من خلال التصفح والتواصل على الإنترنت.

قدم استخدام الإنترنت تحديات مختلفة لموضوع حماية الخصوصية، تختلف أنواع القوانين المختصة بالخصوصية في الفضاء الرقمي فهي تتراوح بين حماية البريد الإلكتروني، وفرض قيود على نشر بيانات التواصل الاجتماعي، ومتابعة نشاط متصفح الإنترنت والمخالفات للبيانات المحفوظة.

وتندد مؤشرات حقوق الإنسان العربية في مجالات عدة وتراءى للبعض أن ما يشهده العالم من تطور تكنولوجي بات من السهل لأي مستفيد عربي أن يهضم تلك المخرجات التقنية الحديثة دون الإصابة بعسر في الهضم.... ولعله يخيب ظني إذ أتوقع تدني مؤشر حقوق الإنسان من المعلومات، المعلومة التي أصيبت بانتكاسة اقتصادية شأنها شأن السلعة سواء في إنتاجها أو تسويقها أو جودتها، إلا أن الخطر الأكبر الذي يحيق بأمن المعلومات هو تفريغها من

مضمونها وقيمتها والقدرة على حمايتها، ذلك أن الفرد العربي اعتاد على التلقين التقني دونما تفعيل أو مشاركة.

ومهما تكن الطريقة التي تجمع المعلومات بواسطتها فإنه يمكن الجزم بأن استخدام شبكة الإنترنت ولو لفترة قصيرة قد يؤدي إلى تجميع معلومات وبيانات شخصية متعددة عن المستخدم التي قد تستغل كلها أو جزء منها في تكوين صورة جانبية عن مستخدمي الشبكة، وبالتالي فإنها تستغل في مراقبتهم.

فمما سبق يتبن لنا أن هناك تحديات جديدة أوجدتها شبكة الإنترنت في مواجهة خطط حماية الخصوصية أو الحياة الخاصة. فهي زادت من كمية البيانات المجمعة والمعالجة والمنشاة، وأتاحت عولمة المعلومات والاتصالات، وبالتالي فقدان المركزية وآليات السيطرة والتحكم.

وكذلك أن تهديد التطور التكنولوجي أو المعلوماتي للأفراد في حياتهم الخاصة أصبح أمرا مدركا ومعروفا، حيث استطاع التغلب على عوائق المسافة والظلام والموانع المادية، وتجاوز عقبة الزمن.

التوصيات

لم تعد المعلومات مادة البحث العلمي فقط، أو مادة التعليم بمراحله، والتدريب وتأهيل الموظفين واستراتيجيات القيادة والإدارة، وعناصر المنافسة في الإنتاج، وخطط التسويق والإعلان، واستراتيجيات تقديم الخدمات، بل أصبحت محددة الفعالية والقدرة لكل ذلك وغيره، فلا عجب إذا أن تمثل تكنولوجيا المعلومات المرتكز الاستراتيجي في خطط البناء والتنمية، وأن تصبح وسائلها – إن في حقل الحوسبة أو حقل الاتصال أو حقل المعطيات – مادة مشروعات الاستثمار الحيوية، وأن تصبح الإنترنت في أيامنا هذه - وهي واسطة مجمعة لوسائل التقنية العالية - مخازن لمليارات (الصفحات) من المعلومات والوثائق السياسية والتاريخية والتجارية والثقافية والعلمية والعسكرية والجغرافية والسياحية والقانونية وغير ذلك، وبيئة لملايين المواقع الخدمية والتجارية وغير الربحية والحكومية والشخصية، ولا عجب أن يتسابق القاصي والداني إلى احتلال موقع ضمن هذه الشبكة، من الإنسان الفرد إلى أعظم مؤسسات علوم الفضاء، ومن المؤسسات والهيئات الأهلية إلى الحكومات والمنظمات الدولية، إن الأفكار هي التي تسهم في خلق مجتمع متطور ولولا مثل هذه الأفكار وتراكم البيانات وتسلسلها لما وصل الشخص إلى كثير مما نتج من دراساته ولما كنا نناقش الآن مثل هذا الموضوع، ولكن لاستغلال العقل البشري ولتعمير الأرض يجب وضع إطار لحماية البيانات والمعلومات، ولذلك تعد البيانات الشخصية عنصرا من عناصر حماية السرية الشخصية واحترام الحياة الخاصة يتعين أن تخضع من حيث نطاق الحماية لما خضعت له عناصر حماية الخصوصية المادية، المسكن والمراسلات وغيرها.

علما بأن المعلومات ككيان معنوي لها ذات القيمة الاقتصادية للمال المادي، يتعين أن تخضع لأحكامه وتعامل تماما كما يعامل، فتحيطها حماية الحقوق ذاتها المقررة على المال المادي ويعترف لها بذات المصالح التي يعترف بها

القانون للمال المادي وفي نطاق التصرفات المدنية والتجارية، فإن السلوكيات والتصرفات القائمة في البيئة الرقمية (بيئة الكمبيوتر والإنترنت) يتعين أن تكون مقبولة ومعترف بها تعبيرا عن الإرادة وعن الالتزام القانوني تماما كتلك التصرفات المعتبرة والمقبولة في البيئة الحقيقة متى ما تحقق لها عنصر القدرة على التعبير بشكل صحيح منتج لأثره.

وفي نطاق الحماية الجنائية يتعين الإقرار بصلاحية المعلومات كمحل للحماية من أنشطة الاعتداء كافة، تماما كما المال المادي المحمي ضمن نصوص وقواعد حماية الأموال، ويتعين الاعتراف لمحيط المعلومات ووعائها التقني بالصفة المقبولة لخضوعه للتصرفات التي ترتكب في بيئة المحرر الكتابي والمستندات الخطية. ويتعين المساواة بين السلوكيات المادية في انتهاك السرية وبين السلوكيات المعنوية في انتهاك الخصوصية.

إن محل الجريمة المعنوي له ذات القيمة المعترف بها للمحل المادي للجريمة، والسلوك المعنوي للجريمة تقوم به الجريمة تماما كما تقوم بالسلوك المادي فعلا وتركا.

إن قواعد الضبط والتفتيش في البيئة الرقمية يتعين أن تتناسب مع مميزات هذه البيئة تماما كما تناسبت قواعد الضبط والتفتيش في الوسط المادي مع مميزات وسلوكيات هذا الوسط.

الأدلة ذات الطبيعة الإلكترونية يتعين مساواتها بالأدلة ذات الطبيعة المادية - الأدلة القائمة على الكتابة والورق - من حيث المقبولية والحجية.

كلما كان التصرف المادي في البيئة الواقعية محل اعتبار يتعين الاعتراف بما يقابله من تصرف معنوي في البيئة الرقمية، فالتوقيع الإلكتروني يقتضي مساواته بالتوقيع المادي. والتصديق الإلكتروني يتعين مساواته بالتصديق المادي، وهكذا، شريطة أن تحقق البيئة الرقمية من حيث المعايير والإجراءات المتصلة بالسلوكيات المعنوية أو سلوكيات البيئة الافتراضية ما يوفر الثقة التي تحلت بها السلوكيات المادية.

إن البيئـة الرقميـة متـى مـا تحقـق نمـط ومعيـار إجـرائي يكفـل لهـا الموثوقيـة والثقـة بالسـلوك في بيئتهـا والاطمئنـان للدليـل المسـتخلص مـن وسـائلها يتعـين أن تعامل كالبيئـة الحقيقـة، وفي نطاقهـا يكـون الحـق محـل اعتراف وتكـون المصلحة موضـع تقدير وتكـون القاعـدة القانونيـة منطقيـة إذا لم تقبـل تمييـزا بـين بيئتين توفر لهـما ذات المعيار مـن حيـث الثقـة وذات العنـاصر مـن حيـث الاطمئنان.

إن المعلومـات بذاتهـا وبمـا يتصـل بهـا مـن سـلوكيات متـى مـا تحقـق الاعـتراف القانـوني بكيانهـا والاعـتراف بمـا يتصـل بهـا مـن تصرفـات ومـا تنشـئها التصرفـات هـذه مـن أثـر ونتائـج ومسـؤوليات، ومـا يتعلـق بهـا مـن حقـوق ومصالـح، حققـت الأسـس القانونيـة المقـر بهـا ضمـن قواعـد كافـة فـروع التشريـع الدسـتورية والمدنيـة والتجاريـة والماليـة والإداريـة والجزائيـة وتشريعـات حمايـة المسـتهلك، المتعلقـة بالتصرفـات المادية والمحـل المـادي والآثـار الناتجـة عـن هـذه السـلوكيات والمراكـز القانونيـة الناشـئة عنهـا.

إن المعلومـات مـال، والتصرفـات المعلوماتيـة ذات وجـود وأثـر، فـلا يتعـين عندها أن تحـرم مـن التنظيـم التشريعـي لأنهـا لـدى الكثيرين افـتراض ووهم. وبالوقت نفسـه لا يتعـين أن تشـقى القواعـد القائمـة في ليّ النصـوص وتطويـع النظريـات القائمـة لتسـتوعب المعلومـات خاصـة بعـد أن تحقـق أثرهـا كعـماد للاقتصـاد الرقمـي، ويتعـين أن تصـاغ النظريـات بمرونـة تسـتوعب القـادم الجديـد في عـصر المعلومـات ووسـائلها فتحظـى بشـمولية المعالجـة لتحقـق سرعـة الاسـتجابة في مرحلـة أصعـب مـا فيهـا إدراك سرعـة التغـير وولادة الأنمـاط المسـتجدة.

وعليـه فنـوصي بدراسـة تشريعات قانونيـة خاصة في البيئـة العربية توفـر الحماية القانونيـة للبيانـات أيـاً كان وسـيط نقلهـا ومعالجتهـا وكذلـك إثـراء البيئـة القائمـة عـلى تنفيـذ تلـك القوانـين حتـى نجـد جـدوى من سـن مثـل هـذه القوانين.

وبمـا أن البيئـة الإلكترونيـة بيئـة منفتحـة لا تسـيطر عـلى وجودهـا أمـة بعينهـا بـل إنهـا لا تملـك مثـل هـذه السـيطرة، نجـد ضرورة وضـع آليـة عالميـة موحـدة

المبادئ والتفسيرات لوضع إطار عادل لحماية البيانات الشخصية، إذ أن تطبيق قانون وطني على مثل هذه الإشكاليات قد يعيق توفير الحماية اللازمة ولإحكام السيطرة على تدفق البيانات من دولة إلى أخرى يجب وجود آلية جامعة مطبقة تطبيق عالمي لفرض مثل هذه السيطرة وإلا سوف يجد دائما المعتدي على البيانات ملاذاً آمناً في إحدى الدول التي لا تطبق القوانين أو كالتي تواجه قصوراً تشريعيا في هذا المجال.

فنرى أن التحرك التشريعي الدولي هو الملاذ وطوق النجاة للبيانات الشخصية عبر الإنترنت وذلك لتوفير القدر المطلوب من الحماية وتفادي آثار المعالجة غير المشروعة أو تعدي أغراض المعالجة المسموح بها.

و بدون ذلك سيظل الحصول على المعلومات والبيانات بغير قيد حاكم أو رادع.

كمتطلب أول لاستشراف آفاق المستقبل نحو مجتمع المعلومات في الوطن العربي، ينبغي إعداد المجتمع العربي وفق ما يلي:

1. اعتبار تهيئة المجتمع العربي لمتطلبات مجتمع المعلومات قضية ثقافية ذات أولية أولي، باعتبار أن العصر المقبل هو عصر المعلومات.
2. ضرورة عمل المؤسسات الثقافية الوطنية بالوطن العربي ومنظماتها علي حث مؤسسات التعليم الرسمي علي سرعة التجاوب مع متطلبات الثورة الإلكترونية.
3. ثمة ضعف في الهياكل السياسية لتقنية المعلومات في معظم البلدان العربية سببه قلة المتخصصين وقلة الذين يؤهلون للمستقبل التقني المعلوماتي يقابل ذلك أن الإنتاج المعرفي تتضخم في العالم بشكل يزيد علي سرعة المتواليات الهندسية. حيث لابد من البدء الفوري بإعداد الهياكل المتخصصة اللازمة.
4. من الأهمية بمكان مواجهة المشاكل المزمنة في تحقيق تكامل معلوماتي

عـربي نتيجـة للحـدود المغلقـة وعـدم وجـود المؤسسـات العربيـة بالسرعـة التـي تفرضهـا الديناميكيـة للثـورة الإلكترونيـة.

5. لابـد مـن التركيـز عـلي الجانـب التعليمـي والتربـوي وعـدم الاكتفـاء بالتعليـم الرسـمي، بـل يجـب أن يشـمل ذلـك التعليـم الـذاتي والتعليـم المسـتمر ومواكبـة خطـط التعليـم لخطـط التنميـة، فالمخططـون لعمليـات التنميـة لا يولـون تقنيـة المعلومـات أي اهتـمام وخاصـة في التربيـة.

6. ضرورة الإسراع في تفعيـل – ولا أقـول إدخـال - دور الحاسـب في نظـم التعليـم الرسـمي، مـع مراعـاة تجـارب الـدول التي سـبقتنا في هـذا الخصوص.

7. لابـد مـن تشـجيع إنتـاج برامـج تعليميـة للحاسـب باللغـة العربيـة وجـذب أكـبر قـدر مـن القـدرات والمواهـب العربيـة لإتمام ذلـك، وربـط إدخـال الحاسـب في نظـم التعليـم الرسـمي بمعالجـة مشـاكل أخـري بـه مثـل الاهتـمام بالـتراث، ومشـاكل تدريـس اللغـة العربيـة للصغـار.

8. ضرورة تغيـير الفلسـفة التعليميـة مـن الأسـلوب التلقينـي الـصرف إلي أسـلوب يشـجع عـلي تنميـة قـدرات حـل المشـكلات والملفـات الابتكاريـة والفنية.

9. توفـير الإطـار الـلازم لتعميـق التفكير حـول المفاهيم الحديثـة لإدارة المعلومات مثـل: مؤشرات الأداء، الجودة الشـاملة، نمـوذج الامتياز.

10. فهـم آخـر المسـتجدات في مجـال إدارة المعرفـة وانعكاسـاتها عـلى خدمـات المكتبـات ومراكـز المعلومـات، والتعـرف عـلى التجـارب العربيـة والأجنبية في هـذا المجال.

11.دراسة واقع مرافق المعلومات العربية وتبادل الآراء حول سبل مواكبة التطورات الحاصلة في مسائل إدارة المعرفة والجودة الشاملة.

12.ضبط جودة خدمات المعلومات في العصر الإلكتروني: قياس أداء المجموعات والإجراءات الفنية والخدمات الموجهة لجمهور المستفيدين كالاهتمام بالجودة الشاملة في إدارة مؤسسات المعلومات في الوطن العربي: من الحوافز والامتياز والإنتاجية.

13.إدارة الموارد البشرية في مرافق المعلومات: إعادة تعريف وظائف المتخصصين في المعلومات ومؤهلاتهم. مفهوم القيادة leadershipفي إدارة مرافق المعلومات، وتأهيل الأفراد والمؤسسات في ظل المنافسة. (27)

14.وضع تشريعات حازمة لإلزام دور النشر والجامعات ومراكز الأبحاث برقممة كل ما سبق ونشرته على الأقل خلال العشرة سنوات السابقة

15.ضرورة وجود جهة مسؤولة عن مشروع الرقمنة ومراقبتها.

ولقد أصبحت مسألة الحماية القانونية - إلى جانب الحماية التقنية - للبيانات الشخصية، ومن العوامل الرئيسة في المناشدة بضرورة وأهمية توفير حماية تشريعية وسن قوانين في هذا الحقل، وأصبحت محل اهتمام دولي وإقليمي ووطني وكذلك ضرورة تقنين قواعد جديدة لمكافحة الجرائم المعلوماتية؛ تأخذ بعين الاعتبار الطبيعة الخاصة لهذه الجرائم ولاسيما فيما يتعلق بالإثبات في الدعاوى الناشئة عن هذه الجرائم؛ سواء في ذلك الدعاوى الجنائية والمدنية والتأديبية.

كما ينبغي تعديل قواعد الإجراءات الجنائية لتتلاءم مع هذه الجرائم، وضرورة التنسيق والتعاون الدولي قضائيا وإجرائيا في مجال مكافحة

الجرائـم المعلوماتيـة وبالتـالي ضرورة تخصيص شرطة خاصة لمكافحة الجرائـم المعلوماتية؛ وذلـك مـن رجـال الشرطة المدربين عـلى كيفيـة التعامل مع أجهزة الحاسـوب والإنترنت.

ويتعـين تدريـب وتحديـث رجـال الادعـاء العـام - أو النيابـة العامـة - والقضـاء بشـأن التعامـل مـع أجهـزة الحاسـوب والإنترنـت. بالإضافـة إلى أنـه ينبغـي أن تنـص التشريعـات العربيـة عـلى اعتبـار أن الإنترنـت يعتـبر وسـيلة مـن وسـائل العلانيـة في قانـون العقوبـات والقوانـين ذات الصلـة بالجرائـم المعلوماتيـة ؛ مـع الأخذ بعـين الاعتبار أن الإنترنـت أوسـع انتشـارا مـن سـائر وسـائل النـشر والعلانيـة الأخـرى.

و يلـزم تعديـل قوانـين ونظـم الإجـراءات الجزائيـة (الجنائيـة)؛ بالقـدر الـذي يسـمح ببيـان الأحـكام الـلازم اتباعهـا حـال التفتيـش عـلى الحاسـبات وعنـد ضبـط المعلومـات التـي تحتويهـا وضبـط البريـد الإلكـتروني حتـى يسـتمد الدليـل مشروعيتـه.

ينبغـي أن يسـمح للسـلطات القائمـة بالضبـط والتحقيـق بضبـط البريـد الإلكتروني وأيـة تقنيـة أخـرى قـد تفيـد في إثبـات الجريمـة والحصـول عـلى دليـل؛ والكشـف عـن الحقيقـة.

و كذلـك أن تمتـد إجـراءات التفتيـش إلى أيـة نظـم حاسـب آلي أخـرى؛ يمكـن أن تكـون ذات صلـة بالنظـام محـل التفتيـش وضبـط مـا بهـا مـن معلومـات، ويشـترط في هـذه الحالـة أن يكـون هـذا الإجـراء ضروريـا، والقاعـدة العامـة - في هـذا الشـأن - الـضرورة تقـدر بقدرهـا.

ويتعـين أن تكـون للسـلطات القائمـة بالضبـط والتفتيـش: سـلطة توجيـه أوامـر لمـن تكـون لديـه معلومـات خاصـة للدخـول عـلى مـا يحويـه الحاسـب الآلي والإنترنـت مـن معلومـات للإطـلاع عليهـا.

كـما نشـير إلى ضرورة النـص صراحـة في القوانـين المنظمـة للإثبـات -

الجنائي والمدني - بما يسمح للقاضي بأن يستند إلى الأدلة المستخرجة من الحاسب الآلي والإنترنت في الإثبات؛ طالما أن ضبط هذه الأدلة جاء وليد إجراءات مشروعة، على أن تتم مناقشة هذه الأدلة بالمحكمة وبحضور الخبير؛ وبما يحقق مبدأ المواجهة بين الخصوم.

بالإضافة إلى اعتبار نشر وطباعة الصور الجنسية عن طريق الإنترنت مما يدخل ضمن زمرة جرائم الآداب.

وكذلك يتعين النص صراحة على تجريم الدخول غير المصرح به على البريد الإلكتروني لإتلاف محتوياته أو إرسال صور إباحية أو تغيير محتواه أو إعاقة الرسائل أو تحويرها عبر الإنترنت.

ونشير إلى ضرورة سن التشريعات لمكافحة جرائم الإنترنت، وذلك بإدخال كافة صور السلوك الضار والخطر على المجتمع التي يستخدم فيها الإنترنت.

بالإضافة إلى ضرورة نشر الوعي بين صفوف المواطنين - ولاسيما الشباب - بمخاطر التعامل مع المواقع السيئة علي شبكة الإنترنت؛ مع ضرورة نشر الوعي المجتمعي بالمخاطر النفسية والاجتماعية وغيرها الناجمة عن الاستخدامات غير الآمنة للإنترنت وتكثيف التوعية عن الآثار السلبية الصحية المترتبة عن الممارسات الجنسية الشاذة ومعاشرة البغايا؛ وذلك بأسلوب غير مباشر من خلال المواد الدرامية.

ومن الممكن تعزيز التعاون والتنسيق مع المؤسسات الدولية المعنية بمكافحة الجرائم المعلوماتية؛ وخصوصا الإنتربول؛ وفي هذا المقام من الممكن أن تنضم الدول العربية إلى الاتفاقيات الدولية الخاصة بمكافحة جرائم الإنترنت، وخاصة المعاهدة الدولية لمكافحة جرائم المعلوماتية والإنترنت والعمل على دراسة ومتابعة المستجدات على الساحة العالمية.

ونأمل أن تسعى الدول العربية إلى إنشاء منظمة عربية تهتم بالتنسيق

في مجال مكافحة الجرائم المعلوماتية عبر الإنترنت؛ مع تشجيع قيام اتحادات عربية تهتم بالتصدي لجرائم الإنترنت وتفعيل دور المنظمات والإدارات والحكومات العربية في مواجهة هذه الجرائم عن طريق نظام الأمن الوقائي؛ ويا حبذا لو تم إنشاء شرطة عربية تهتم بمكافحة الجرائم المعلوماتية.

وأن يتم التنسيق بين دان حماية الخصوصية في البيئة الرقمية عملية وليست مجرد إجراء، بمعنى أنها تنطلق من رؤية محددة المعالم واضحة الأهداف وتكون مخرجاتها حزمة من الوسائل والإجراءات في ميادين التقنية والقانون وإدارة النظم التقنية، وبوصفها عملية تكاملية، فإنها محكومة بإستراتيجية تحدد عناصر الحماية ونطاقها، لهذا فإن من الخطأ القاتل مجرد الاعتقاد أن استخدام بعض التقنيات التي تحمي البيانات الشخصية قد حقق حماية للخصوصية، ومن الاعتقادات الخاطئة أيضا أن مجرد التزام جهات جمع البيانات باحترام الخصوصية يحقق الحماية أو يحقق مساءلتها إن حصل إخلال، والخطأ الأكثر خطورة إغفال أهمية الحماية القانونية الشمولية وتكاملها مع الحماية التقنية والخطوات التنظيمية.

قائمة المراجع

أولاً: المراجع باللغة العربية:

1. المراجع العامة

1. ابن منظور: لسان العرب، ط 1، منشورات مطبعةبولاق، جزء 8

2. اسامة احمد: جرائم الحاسب الالي والانترنيت- ط -1 دار وائل للنشر- الاردن- 2001.

3. اسامة عبد الله قايد: المسؤولية الجنائية للطبيب عن افشاء سر المهنة- دار النهضة العربية- القاهرة- 2000

4. د.السنهوري: نظرية العقد، الجزء الأول، ط1، 1934 م، القاهرة

5. د.إبراهيم الدسوقي أبو الليل: الجوانب القانونية للتعاملات الالكترونية، مجلس النشر العلمي، الكويت، 2003

6. إسماعيل غانم: النظرية العامة للالتزامات، القاهرة، 1966

7. د.أبو العلا النمر: الحماية الوطنية للملكية الفكرية في ظل اتفاقية الجوانب المتصلة بالتجارة من حقوق الملكية الفكرية.دار أبو المجد للطباعة، الطبعة الثانية.

8. أحمد جاد منصور: ضمانات الحق في حرمة الحياة الخاصة، المنظمة العربية للتنمية الإدارية، 2013.

9. د.أحمد عبد الكريم سلامة: القانون الدولي الخاص النوعي (الالكتروني، السياحي، البيئي)، دار النهضة العربية، ط1، 2002

10. أحمد فضل شبلول: حول الملكية الفكرية وحقوق المؤلف على شبكة الإنترنت، 2007.

11. أسامة أبو الحسن مجاهد: التعاقد عبر الانترنت، دار الكتب القانونية، المحلة الكبرى، 2002.

12. أسامة أبو الحسن مجاهد: خصوصية التعاقد عبر الانترنت، دار النهضة العربية، 2000.

13. أمير فرج يوسف: عالمية التجارة الإلكترونية و عقودها، المكتب الجامعى الحديث، الإسكندرية، 2009.

14. د.جميل عبد الباقي الصغير: الجنائية لقرصنة البرامج التلفزيونية المدفوعة- دار النهضة العربية- القاهرة- -2001.

15. الجوانب الإجرائية للجرائم المتعلقة بالإنترنت، دار النهضة العربية، القاهرة 1998م.

16. د.حسام الدين الأهواني: الحق في إحترام الحياه الخاصه، الناشر دار النهضه العربيه، (1978).

17. د.حسام شوقي: حماية و أمن المعلومات على الإنترنت، دار الكتب العلمية 2004.

18. خالد مصطفي فهمي: الحماية القانونية لبرامج الحاسب الآلي، الإسكندرية، دار الجامعة الجديدة للنشر، سنة 2005 م.

19. خالد ممدوح إبراهيم: إبرام العقد الإلكتروني، (دراسة مقارنة)، دار الفكر الجامعي، الإسكندرية 2006.

20. إبرام العقد الالكتروني، دار الفكر الجامعي، 2006.

21. د.رأفت رضوان: عالم التجارة الإلكترونية، المنظمة العربية للتنمية الإدارية، القاهرة1999.

22. رشاد عبد الله: الإنترنت في مصر والعالم العربي، ط 1، آفاق للنشر و التوزيع، 2005.

23. سعيد عبد اللطيف: علي الجرائم الناشئة عن استخدام الحاسب الآلي كلية الشريعة والقانون القاهرة1999.

24. سميحة القيلوبي: "الملكية الصناعية"، دار النهضة العربية، (بدون سنة الطبع).

25. سمير حامد عبد العزيز الجمال: التعاقد عبر تقنيات الاتصال الحديثة، الطبعة الأولى، دار النهضة العربية، القاهرة 2000.

26. شحادة غريب شلقامي: برامج الحاسب الآلي والقانون، القاهرة، دار النهضة العربية، سنة.

27. شريف محمد غنام: التنظيم القانوني للإعلانات التجارية عبر شبكة الانترنت، دار الجامعة الجديدة، الإسكندرية، ص: 149، 2008م.

28. د.صالح جواد كاظم: التكنولوجيا الحديثة والسرية الشخصية"، الطبعة الاولى، بغداد، 1991.

29. عن التكنولوجيا الحديثة والسرية الشخصية (مباحث في القانون الدولي)، الطبعة الأولى، دار الشؤون الثقافية العامة، بغداد، 1991.

30. عباس العبودي: التعاقد عن طريق وسائل الاتصال الفوري وحجيتها في الاثبات المدني، دار الثقافة للنشر والتوزيع، عمان، 1997.

31. عباس محمد حسني: الملكية الصناعية والمحل التجاري، عمان، دار الفرقان، سنة 1994.

32. د.عبد الاحد جمال الدين: النظرية العامة للجريمة- دار الثقافة الجامعية- القاهرة- 1996.

33. عبد الحميد بسيوني: الحماية من أخطار الأنترنت، دار الكتب العلمية، 2003.

34. عبد الفتاح بيومي حجازي: مكافحة جرائم الكمبيوتر والانترنت في القانون العربي النموذجي، ط1، دار الفكر الجامعي، الإسكندرية، 2006.

35. الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنت - دار الكتب القانونية - 2002.

36. عبد الفتاح مراد: شرح جرائم الكمبيوتر والأنترنت، دار الكتب والوثائق المصرية.

37. د.عصام أحمد البهجي: حماية الحق في الحياة الخاصة في ضوءحقوق الإنسان، الدار العربية للنشر و التوزيع، 2000.

38. علي عبد القادر القهوجي: الحماية الجنائية لبرامج الحاسب الآلي، الإسكندرية، 1997

39. عمر الفاروق الحسيني: المشكلات الهامة في الجرائم المتصلة بالحاسب الآلي وأبعادها الدولية، القاهرة، 1992.

40. عمر أبو بكر بن يونس: الجرائم الناشئة عن استخدام الإنترنت - دار النهضة العربية، القاهرة 2004.

41. عمر محمد بن يونس: أشهر المبادئ المتعلقة بالانترنت لدى القضاء الأمريكي، بدون ناشر، 2004م.

42. عمرو احمد حسبو: حماية الحريات في مواجهة نظم المعلومات- دار النهضة العربية- القاهرة- 1985.

43. قانون البرمجيات، دار الكتاب الحديث، القاهرة، 2001فاروق علي حفناوي.

44. فهمي، خالد مصطفي: الحماية القانونية لبرامج الحاسب الآلي، الإسكندرية، دار الجامعة، الجديدة للنشر.

45. فيصل محمد محمد علد العزيز: الحماية القانونية لعقود التجارة الالكترونية، دار النهضة العربية، القاهرة، 2008م.

46. لطفي، محمد حسام: الحماية القانونية لبرامج الحاسب الالكتروني، دار الثقافة للطباعة والنشر، سنة 1978.

47. ماجد عمار: المسئولية القانونية الناشئة عن استخدام فيروس برامج الكمبيوتر ووسائل حمايتها، دار النهضة العربية، القاهرة، 1989.

48. مأمون محمد سلامة: قانون العقوبات، القسم الخاص، ج1، دار الفكر العربي، 1982-1983.

49. محمد الفيومي: مقدمة الحاسبات وتشغيل الحاسبات الصغيرة، الإسكندرية، المكتب الجامعي الحديث، سنة 1998.

50. د.محمد امين الشوابكة: "جرائم الحاسوب والانترنت الجريمة

المعلوماتية "دار الثقافة للنشر والتوزيع الطبعة الاولى - الاصدار الثاني 2007.

51. محمد أمين الرومي: التعاقد الالكتروني عبر الانترنت، دار المطبوعات الجامعية، الإسكندرية، 2004.

52. التعاقد الإلكتروني عبر الانترنت، الطبعة الأولى، دار المطبوعات الجامعية، الإسكندرية 2004.

53. جرائم الكومبيوتر والانترنت، دار المطبوعات الجامعية 2003.

54. محمد حسام لطفي: الحماية القانونية لبرامج الحاسب الالكتروني، جامعة بني سويف، 1987.

55. "الحماية القانونية لبرامج الحاسب الالكتروني" دار الثقافة للطباعة والنشر القاهرة، الطبعة الأولى 1978

56. محمد حسن قاسم: التعاقد عن بعد، دار الجامعة الجديدة للنشر، الإسكندرية، 2005.

57. محمد حسني عباس: الملكية الصناعية أو طريق انتقال الدول النامية إلى عصر التكنولوجيا"، المنظمة العالمية للملكية الفكرية، جنيف 1967.

58. د. محمد حسين منصور: المسئولية الالكترونية، دار الجامعة الجديدة، الإسكندرية، 2003.

59. المسؤولية الالكترونية، دار الجامعة الجديدة للنشر، الإسكندرية، 2003.

60. المسؤولية الالكترونية، منشأة المعارف، الإسكندرية، 2006.

61. محمد سامي الشوا: ثورة المعلومات وانعكاساتها على قانون العقوبات، دار النهضة العربية.

62. محمد عبد اللطيف عبد العال - الجرائم المادية وطبيعة المسؤولية الناشئة عنها- دار النهضة العربية- القاهرة- 1997.

63. محمد عبد المحسن: المقاطع- حماية الحياة الخاصة للافراد وضمانا في مواجهة الحاسوب الالي- ذات السلاسل للطباعة والنشر- الكويت 1992.

64. محمد عبد الظاهر حسين: المسئولية القانونية في مجال شبكات الانترنت، دار النهضة العربية، القاهرة، 2004/2003.

65. محمد على العريان: الجرائم المعلوماتية، دار الجامعة الجديدة للنشر، الإسكندرية، 2004.

66. محمد على فارس الزغبي: الحماية القانونية لقواعد البيانات، منشأه المعارف، 2010.

67. محمود عبد الرحمن محمد: نطاق الحق في الحياة الخاصة، دار النهضة العربية، 1995.

68. محمود نجيب حسني: شرح قانون العقوبات – القسم الخاص، دار النهضة العربية، 1994.

69. د.مدحت عبد الحليم رمضان: الحماية الجنائية للتجارة الإلكترونية، دار النهضة العربية 2001.

70. مدحت محمد محمود عبد العال: مدى خضوع برامج الحاسب الآلي للحماية المقررة للمصنفات،، الأدبية في ظل قانون حماية حق المؤلف، القاهرة، دار النهضة العربية.

71. مصطفى محمد موسى: أساليب إجرامية بالتقنية الرقمية (ماهيتها و مكافحتها)، دار الكتب القانونية، 2005.

72. ممدوح محمد علي مبروك: مدى حجية التوقيع الإلكتروني في الإثبات، دار النهضة العربية، القاهرة.

73. مينشار: الانترنت والقانون، منشورات مون كريستان، 1999 باريس.

74. محمدسامي الشوا: ثورة المعلومات وانعكاساها على قانون العقوبات - دار النهضة العربية- القاهرة1994-.

75. نائلة عادل محمد فريد: جرائم الحاسب الآلي الاقتصادية، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت – لبنان، 2005.

76. نزيه محمد المهدي: الإلتزام قبل التعاقدي بالإدلاء بالبيانات المتعلقة بالعقدو تطبيقاتها على بعض أنواع العقود، دار النهضة العربية، 2000.

77. نعيم مغبغب: مخاطر المعلوماتية والانترنيت- دار النهضة العربية- القاهرة- 1998.

78. د.هدى حامد قشقوش: جرائم الحاسب الالكتروني في التشريع المقارن- دار النهضة العربية- القاهرة- 1992.

79. جرائم الحاسب الالكتروني في التشريع المقارن- دار النهضة العربية- القاهرة.

80. د.هشام فريد رستم: قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات حديثة، أسيوط، 1992.

81. د.هلالي عبد اللاه احمد: تفتيش نظم الحاسب الالي، ط1، دار النهضة العربية، القاهرة 1997.

82. هلال عبد اللاه احمد: التزام الشاهد بالاعلام في الجرائم المعلوماتية - ط-1 دار النهضة العربية- القاهرة- 1997.

83. يوسف احمد النوافلة: الحماية القانونية لحق المؤلف، دار الثقافة للنشر والتوزيع، الأردن، ط2004.

84. يوسف الشيخ: حماية الحق في حرمة الأحاديث الخاصة، دار الفكر العربي، 2001.

85. يونس عرب: دور حماية الخصوصية في تشجيع الاندماج بالمجتمع الرقمي.

86. التدابير التشريعية العربية لحماية المعلومات والمصنفات الرقمية، ورقة عمل مقدمة امام:-الندورة العلمية الخامسة حول دور التوثيق والمعلومات في بناء المجتمع العربي – النادي العربي للمعلومات – دمشق، 2013

87. الكتاب الثاني من موسوعه القانون و تقنيه المعلومات -الخصوصيه و حمايه البيانات في العصر الرقمي، 2002

88. الخصوصية وحماية البيانات في البيئة العربية.دائرة المكتبة الوطنية، 2002.

89. الكتاب الثاني دليل امن المعلومات والخصوصية، ج1، جرائم الكمبيوتر والانترنت ط1، منشورات اتحاد المصارف العربية، بيروت.

90. الحقائق الخفية في دعاوى الملكية الفكرية، نسخه إلكترونيه، 2010.

2- الرسائل العلمية:

1. انتصار عباس ابراهيم: اثر وسائل الإتصال في خدمات المكتبات ومراكز المعلومات. الخرطوم: جامعة النيلين، 2005.

2. أحمد حسام طه: الجرائم الناشئة عن استخدام الحاسب الآلي، رسالة دكتوراه، كلية الحقوق، جامعة طنطا.

3. أحمد خالد العجلوني: التعاقد عن طريق الانترنت، رسالة ماجستير، 2002.

4. بشار طلال مومنى:مشكلات التعاقد عبر الانترنت، رسالة دكتوراة، كلية الحقوق، جامعة المنصورة، 2003.

5. سليمان بن مهجع العنزي: وسائل التحقيق في جرائم نظم المعلومات، رسالة ماجستير في العلوم الشرطية، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، الرياض 2003م.

6. صلاح الدين مرسي: الحماية القانونية لحق المؤلف في التشريع الجزائري، رسالة دكتوراه في القانون، كلية الحقوق جامعة بن عكنون، الجزائر، 1988م.

7. طارق أحمد سرور: الحماية الجنائية لأسرار الأفراد في مواجهة النشر، رسالة دكتوراه، دار النهضة العربية، القاهرة، سنة 1991 م.

8. عبد الصادق، محمد سامي: حقوق مؤلفي المصنفات المشتركة، رسالة دكتوراه، جامعة القاهرة، سنة 2000 م.

9. عبد الفتاح محمود كيلاني: المسئولية المدنية الناشئة عن المعاملات الالكترونية عبر الانترنت (رسالة دكتوراه)، دار الجامعة الجديدة، الإسكندرية، 2011.

10. عفيفي كامل عفيفي: جرائم الكمبيوتر ودور الشرطة والقضاء، رسالة دكتوراه، كلية الحقوق، جامعة الإسكندرية، 1999.

11. محمد جمال عطية: الشكلية القانونية، دراسة مقارنة، رسالة دكتوراة، كلية الحقوق، جامعة الزقازيق، 1993.

3- الأبحاث و الدوريات:

1. أحمد بدر: مجتمع المعلومات الكونى ومشكلات الخصوصية وأمن المعلومات وحق التأليف.- مجلة مكتبة الملك فهد الوطنية.- مج 3، ع 2 1998م).

2. جمال عبد الله: ندوة المعلوماتية القانونية والقضائية، المركز العربي للدراسات والبحوث القانونية، 1998.

3. جينشار وآخرين: الانترنت والقانون، منشورات مون كريستان، باريس 1999.

4. د.حسام الدين الاهواني: حماية حقوق الملكية الفكرية في مجال الانترنت، ورقة عمل مقدمة الى مؤتمر الملكية الفكرية - جامعة اليرموك - الاردن 10-2000/7/11.

5. خالد محمود إبراهيم: حماية المستهلك في المعاملات الالكترونية، دراسة مقارنة، الدار الجامعية، الإسكندرية، ص 60، 2007.

6. رامي علوان: بحث بعنوان "التعبير عن الإرادة عن طريق الانترنت واثبات التعاقد الالكتروني "، مجلة الحقوق، ع 4، س26، ديسمبر 2002.

7. سعد الحاج بكري: شبكات الاتصال وتوظيف المعلومات في مكافحة الجريمة- المجاة العربية للدراسات الامنية والتدريب- س -6 ع 11).92 - الرياض- 1990.

8. عـادل شـمران الشـمري: الانتهـاك الالكـتروني لخصوصيـة الأفـراد ووسـائل مواجهتـهُ، كليـة القانـون - جامعـة كربـلاء، (2010)

9. عبـد اللـه بـن إبراهيـم النـاصر: "العقـود الالكترونيـة، دراسـة فقهيـة تطبيقيـة مقارنـة " بحـث مقـدم إلى مؤتمـر الأعـمال المصرفيـة الالكترونية بـين الشريعة والقانـون والمقـام بدولـة الإمـارات العربيـة المتحـدة في الفـترة مـن 10 _12 مايو 2003.

10. عثـمان سـعيد المحيـشي: ورقـة عمـل مقدمـة لمنظمـة العربيـة للتنميـة الإداريـة، المؤتمـر الـدولي الأول لقانـون الإنترنـت، 2005.

11. عمـر عدنـان العوبثـاني: في تقريـره "العـرب و التجـارة الإلكترونيـة و مخـاوف الـدوت كـوم " منشـور بالملحـق الإقتصـادي لجريـدة الخليـج الإماراتيـة، العـدد8116.

12. فـؤاد جـمال: إطلالـة عـلى حمايـة حقـوق الملكيـة الفكريـة في مـصر، منشـور ضمـن مجلـة "رسـالة المعرفـة"، مركـز تنميـة البحـوث، المخابـرات العامـة المصريـة، العـدد الثـانى، 2006.

13. لورنـس م. أوليفيـا: أمـن تقنيـة المعلوماتترجمـة محمـد عبـد السـتار، مركـز دراسـات الوحـدة العربيـة، 2011.

14. متـولي عبـد المؤمـن: الجريمـة عـبر الانترنـت، منتـدى جامعـة المنصـورة عـلى النترنـت، 2008، بحـث منشـور عـلى الموقـع: http:// www.f-law.net/ .nedex.php

15. محمـد عبـد المحسـن المقاطـع: حمايـة الحيـاة الخاصـة للأفـراد وضماناتهـا في مواجهـة الحاسـب الآلي، جامعـة الكويـت، 1992.

16. محمـــد واصـــل: الحمايـــة القانونيـــة للمصنفـــات الرقميـــة (برامـــج

الحاسـوب) مجلـة جامعـة دمشـق للعلـوم الاقتصاديـة والقانونيـة - المجلـد 27 - العـدد الثالـث- 2011.

17. محمـود صالـح العـادلي: الجرائـم المعلوماتيـة ماهيتهـا- صورهـا، ورقـة عمـل مقدمـة إلى ورشـة العمـل الإقليميـة حـول تطويـر التشريعـات في مجـال مكافحـة الجرائـم الالكترونيـة التـي أُقيمـت في مسـقط 2-4 ابريـل 2006 بالتعـاون مـع مركـز التميـز العـربي التابـع للاتحـاد الـدولي للاتصـالات.

18. محمـد محيـي الديـن عـوض: مشـكلات السياسـة الجنائيـة المعـاصرة في جرائـم نظـم المعلومـات(الكمبيوتـر) – ورقـة عمـل مقدمـة إلى المؤتمـر السـادس للجمعيـة المصريـة للقانـون الجنـائي – المنعقـد بالقاهـرةفي الفـترة مـن 25- 28 أكتوبـر 1993 م.

19. مفتـاح بوبكـر المطـردي: الجريمـه الإلكترونيـه و التغلـب عـلى تحدياتهـا، ورقـة مقدمـة إلي المؤتمـر الثالـث لرؤسـاء المحاكـم العليـا في الـدول العربيـة بجمهوريـة السـودان المنعقـد في23-25 / 9 / 2012ص24.

20. نبيلـة إسـماعيل رسـلان: المسـؤولية في مجـال المعلومـات والشـبكات، مجلـة روح القوانـين، كليـة الحقـوق، جامعـة طنطـا، العـدد 18، سـنة 1999 م.

21. نضـال الشـاعر: الجـرام المعلومـاتي في وسـائل الاتصـال الالكـتروني"، دراسـة منشـورة في نـشرة المعلومـات القانونيـة الصـادرة عـن جمعيـة علـماء المعلوماتيـة في لبنـان، العـدد 3 آيـار، 2005، دار نـاشرون، بـيروت.

22. نـواف كنعـان: حمايـة حقـوق التأليـف لبرامـج الحاسـبات الالكترونيـة.

23. هاشـم فريـد رسـتم: الجرائـم المعلوماتيـة – أصـول التحقيـق الجنـائي

الفني واقتراح بإنشاء آلية عربية موحدة للتدريب التخصصي – بحثمقدم إلى مؤتمر القانون والكمبيوتر والإنترنت – في (3-1 مايو2000م.

24. يونس عرب: التدابير التشريعية العربية لحماية المعلومات والمصنفات الرقمية، ورقة عمل مقدمة أمام الندوة العلمية الخامسة حول دور التوثيق والمعلومات في بناء المجتمع العربي النادي العربيه، للمعلومات- د مشق .

25. دراسة استقصائية عالمية حول خصوصية الإنترنت وحرية التعبير، سلسلة اليونسكو بشأن حريةالإنترنت 2013/11/28/

26. ندوة اخلاق المعلومات - نادي المعلومات العربي – 16-17 اكتوبر 2002 – عمان – الاردن

27. الخصوصية وحماية البيانات، بحث منشور على شبكة الإنترنت من خلال موقع www.arablaw.

28. داره العامة، العدد 59، سنة 1988 م.

29. رشيد تاز: إعلان طهران،، مطبوعات الأمم المتحده، (2009).

30. الأمم المتحدة - أعمال الأمم المتحدة في ميدان حقوق الانسان - المجلد الأول. منشورات هيئة الأمم المتحدة (رقم المبيع 89 GE-15564 نيويورك، 1990.

ثانيـاً: المراجع باللغـة الإنجليزية:

1. Books

1. Adams، Helen. Privacy in the 21st Century. Connecticut: Libraries Unlimited American Library Association، 2005.

2. Aishankar، K. Cyber Criminology: Exploring Internet Crimes and Criminal behaviour. Boca Raton، FL، USA: CRC Press، Taylor and Francis Group. (Ed.) (2011).

3. Alain Bensoussan Internet، aspects juridiques، éd. Hermes، 1998

4. Albert Gore، Jr.، A Framework for Global Electronic Commerce، July 1، 1997

5. Allen، Julia H The CERT Guide to System and Network Security Practices. Boston، MA: Addison-Wesley. (2001).

6. AmitaiEtzioni The Limits of Privacy، New York: Basic Books.(2000)

7. Andrea Peterson، "Privacy Protections for Cloud E-mail"، Think Progress، (March 20، 2013)

8. Angela Choey Protecting Privacy on the internet: Alegislative Proposal 1997

9. Anne Bliss، Ph.D.، TECHNOLOGY AND

PRIVACY IN THE NEW MILLENNIUM، Ethica Publishing، 2004

10. Arvind Narayanan and VitalyShmatikov ، De-anonymizing Social Networks، The University of Texas at Austin، (2012)

11. Avner Levin، International Comparison of Cyber Crime، PRIVACY AND CYBER CRIME INSTITUTE، 2013

12. Bell، John. Principles of French law (Oxford ; New York: Oxford University Press، 1998)

13. Bernar، MY، Privacy Rights Clearinghouse، a consumer education and privacy rights advocacy organization 2001

14. Branscomb، Anne Who Owns Information?: From Privacy To Public Access". Basic Books (1994)

15. Brendan Sasso and Jennifer Martinez Houseto ConsiderEmailPrivacy Bill، TheHill، 2013

16. Brennan، William. The Quest to Develop Jurisprudence of Civil Liberties in Times of Security. 2007.

17. Brenner، S. "Law in an Era of Smart Technology"، Oxford: Oxford University Press (2007)

18. Brent E. Turvey، Diana Tamlyn، Jerry Chisum

Criminal Profiling: An Introduction to Behavioral Evidence Analysis،، 1 edition، Academic Press Limited 1999

19. Cairns، Walter. Introduction to French law (London: Cavendish، 1995(، see also West، Andrew. The French legal system 2nd ed. (London: Butterworths، 1998

20. Cathy Beagan Flood، Iris Fischer، Nicole Henderson and Pei Li. "Ontario Court of Appeal Recognizes New Privacy Tort".

21. Daniel J. Ryan; Gal Shpantzer. "Legal Aspects of Digital Forensics". (August 2010)

22. David Levi، Computer fraud charges in New York...، PC، Forest Hills، NY (May 2011)

23. Dawn E. Bowman، INTELLECTUAL PROPERTY RIGHTS AND COMPUTER SOFTWARE، DawnSheree @ AOL1996

24. Den، Marc L.، and Stephanie E. Lucas Accidents On the Information Superhighway: On-Line، Liability and Regulation، (1996).

25. Denning، Dorothy E. Concerning Hackers Who Break into Computer Systems (1990).

26. Donegan، Pracilla. "Mining for knowledge."

Grocery Headquarters، February (2000)

27. Donn B. Parker Fighting Computer Crime: A New Framework for Protecting Information،، 1 edition، John Wiley & Sons (1998)

28. Duke، Privacy The Development of a Law and the Legal Theory، UK BOOKs،، (2011)

29. Eagle K. "Potential impact of the HIPAA privacy rule on data collection in a registry of patients with acute coronary syndrome". Arch Intern Med P165 (2005)

30. Easttom C. Computer Crime Investigation and the Law، New Y press، (2010)،

31. Elliott، Catherine. French legal system (Harlow، England: Longman، 2000)

32. EnekenTikk، IP addresses subject to Personal data regulation، Out Law، (2013)

33. Epstein، Michael A. Epstein on Intellectual Property. Aspen Publishers Online (2006).

34. Etzioni، A Communitarianism. In B. S. Turner (Ed.)، The Cambridge Dictionary of Sociology Cambridge، UK: CambridgeUniversity. (2006).

35. Etzioni، A. “Are new technologies the enemy of privacy”، (2007)

36. Fafinski، S. Computer Misuse: Response، regulation and the law Cullompton: Willan (2009)

37. Flaherty، D. "Protecting privacy in surveillance societies": The federal republic of Germany، Sweden، France، Canada، and the United States. Chapel Hill، U.S.: The University of North Carolina Press (1989)

38. Fred H. Cate INFORMATION PRACTICE PRINCIPLES forthcoming in Consumer Protection in the Age of the 'Information Economy (2005)

39. Grabosky، P. Electronic Crime، New Jersey: Prentice Hall،

40. H. Jeff Managing Privacy: Information Technology and Corporate AmericaBookrule، USA، (2001)

41. Harry A. Hammitt، David L. Sobel، and Mark S. Litigation Under the Federal Open Government Laws"(2002)

42. Hazel، Robert. Commentary on The Freedom of Information White Paper، unit-publications (2013)

43. Helft، Miguel and Claire Cain Miller News Analysis: Privacy Law Is Outrun by the Web، (1986)

44. Henrik W.K. Computer crime and other crime against Information Technology In Netherland OKJ Press " R.I.D.P 1993

45. Hoffman، David; Rowe، John Human Rights in the UK: an Introduction to the Human Rights Act 1998 (2nd ed.). Harlow، United Kingdom (2006)

46. Hunton& Williams LLP، New Requirements for Online Privacy Policie، Basic Books (2004)

47. Iris Fischer، Nicole Henderson. Ontario Court of Appeal Recognizes New Privacy Tort".Blake، Cassels&Graydon، (2003)

48. Jain، A.، Hong، L.، &Pankanti، S. "Biometric Identification". Communications of the ACM، (2000)

49. James W.H. McCord and Sandra L. McCord، Criminal Law and Procedure for the paralegal: a systems approach، supra، (2000)

50. James، N، J "Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)"thmases، (2013)

51. Joan E. Rigdon، "Internet Users Say They'd Rather Not Share Their ه Cookies"، 'WALL ST. J.، (Feb. 14، 1996)

52. John، . A. Application of the United States of America privacy laws of January 25، (2013)

53. John C. Yates، Privacy & Data-Mining On The Internet، (1999)

54. John S James and Leslie F Maxwell. A Bibliography of the British Commonwealth of Nations. Second Edition. Sweet & Maxwell. 1957. Volume 2

55. John Shattuck Rights of Privacy، National Textbook Co.، 1977

56. John Waddam، Kelly Harres، Blackstone's Guide to the Freedom of Information Act 2000 oxfordUniversity press، 2010

57. Johnson Deborah، Beauchamp، Bowie، Arnold، ed. "Ethical theory and business". (8th ed.) UpperSaddleRiver (2009)

58. Johnson، Deborah (2009). Beauchamp، Bowie، Arnold، ed. Ethical theory and business. (8th ed. ed.). Upper Saddle River، N.J.: Pearson/ Prentice Hall

59. Julia M. Fromholz The European Union Data Privacy Directive، Berkeley Tech. (2000);

60. Kang Shuhua، Comprehensively building a moderately prosperous society in Crime، Chaniees 1991

61. Kenneth R. Shear، What You Don't Know Can Hurt You: E-Mail Privacy Claims Under the Federal Electronic Communications Privacy Act، LAW OFF. ECON. & MGMT. (1996).

62. KrisanaKitiyadisai، "Privacy Rights and Protection: Foreign Values in Modern Thai Context"، springerlink، March (2005)

63. Laura E. Quarantiello Cyber Crime: How to Protect Yourself from Computer Criminals، Tiare Publications، 1996

64. Litman، Jessica Digital Copyright. Berlin: Prometheus Books.(2000)

65. Lori Andrews، Social Networks and the Death of Privacy، free press (2011)

66. MacDonald، Jones، The Law of Freedom of Information BBC press، (2003)

67. Malcolm Clarke Developing a Standard for Personal Health Devices based on 11073 (ConfProc IEEE Eng Med Biol Soc.(2007)

68. Marc Rotenberg، and Paul M. Schwartz Privacy، Information، and Technology، Aspen Publishers، (2007).

69. Marco، P.M "Personal Health Information Custodians in New Brunswick Exemption Order:". Department of Justice. (2011)

70. Mark K. Smallhouse، Drafting Effective E-Mail Policies، PREVENTIVE L. REP. (1995).

71. McCullagh، Declan; Anne Broache Senate Ratifies Controversial Cybercrime Treaty، UIJ press t 2006

72. McQuade، S. Understanding and Managing Cybercrime، Boston: (2006)

73. McQuade، S..“Understanding and Managing Cybercrime”، Boston: Allyn& Bacon (2006)

74. Mediati، N. The Most Dangerous Places on the Web. PC World، (2010)

75. Mena، Jesús Machine Learning Forensics for Law Enforcement، Security، and Intelligence (2011).

76. Michael، J، "Privacy and human Rights"، An international and comparative study with special reference of development in information technology، (1994)

77. Miller، A “The Assault on Privacy”، Ann Arbor، University of Michigan Press، (1971)

78. Miller، Vincent Understanding digital culture. "Convergence and the contemporary media experience". London: Sage Publications(2011)

79. Moore، R. "Cyber crime: Investigating High-Technology Computer Crime، " Cleveland، Mississippi: Anderson Publishing (2005)

80. Narayanan، A.; Shmatikov، V. "Myths and

fallacies of "personally identifiable information"". Communications، (2010).

81. Parker D.B. “Combattre la crimpinalite in formatiqe” (1985)

82. Paul M. Schwartz Privacy، Information، and Technology، Aspen Publishers، (2006)

83. Paul Taylor Hackers: Crime in the Digital Sublime (November 3، 1999 ed.). Routledge; 1 edition

84. Penenberg، Adam; Cookie Monsters، Slate، (November 7، 2005)

85. Peng، Weihong; Cisna، Jennifer HTTP cookies – “A promising technology"، (2000)

86. Perun، Halyna; Michael Orr، Fannie Dimitriadis "2". Guide to the Ontario Personal Health Information Protection Act. TorontoON، Canada: Irwin Law (2005).

87. Pfleeger، Charles; Pfleeger، Shari Security in Computing (4th ed.). Boston: Pearson Education (2007)..

88. Pieter van Dijk، Godefridus J. H. Hoof، G. J. H. Van Hoof “Theory and Practice of the European Convention on Human Rights”و MartinusNijhoff Publishers، (1998)

89. Popa، C.، et. al.، "Managing Personal Information: Insights on Corporate Risk and Opportunity for Privacy-Savvy Leaders"، Carswell (2012)

90. Quinn، Michael J. Ethics for the Information Age، U.Y.E pub، (2009).

91. Raymond Wacks Privacy: A Very Short Introduction، Oxford: OxfordUniversity Press، 2009

92. Richard T. De George، ". Intellectual Property Rights، " in The Oxford Handbook of Business Ethics، by George G. Brenkert and Tom L. Beauchamp، vol. 1، 1st ed. (Oxford، England: OxfordUniversity Press، n.d.)،

93. Richardson، R. CSI Computer Crime & Security Survey. Computer Security Institute. (2010).

94. Rob Barrass، Lyndsay A. Wasser، "Seclusion intrusion: a common law tort for invasion of privacy". McMillan LLP، (2012)

95. Robert Gellman، Fair Information Practices: A Basic History WDC Pub.، 2008

96. Robert Gellman، Does Privacy Law Work?، Technology and Privacy: "The New Landscape" n.d

97. Roger Clarke Introduction to Dataveillance and Information Privacy، and Definitions of Terms Xamax Consultancy Pty Ltd، 2013

98. Roger Clarke's Privacy and Social Media: An Analytical Framework، "Data Surveillance and Information Privacy" (2013)

99. Roger Clarke's The Nature of the Digital Persona and Its Implications for Data Protection Law (January، for BahcesehirUni، Istanbul (2014)

100. Rouse، Margaret، "Transient cookie session cookie"، (September 2005)

101. Rule، J B. Private Lives and Public Surveillance"، London، Allen Lane، (1973)

102. shraddha، Peter J. Lyons&Co.:LEO Computers (2002)

103. Snell A. "IT security gets personal." Management & Careers Ethica Publishing، (2007)

104. Thomas . Foreign law: current sources of codes and basic legislation in jurisdictions of the world (Littleton، Colo.: F.B. Rothman، (1989)

105. UlserSieber ، legal aspects of computer related crimes، Eu Commission (1998)

106. VinodBangeand Graham Hann An overview of UK dataprotection law، Taylor Wessing(2006)

107. Vivant et lestanc lamy in Droit de Linformatique" paris (1989)

108. Walden، I. Computer Crimes and Digital Investigations، Oxford: OxfordUniversity Press، (2007)

109. Wall، D.S. Cybercrimes: The transformation of crime in the information age، Cambridge: Polity(2007)

110. Wall، D.S. Cybercrimes: The transformation of crime in the information age، Cambridge (2007)

111. Wendy Benjamin Jersey:"Data Protection In Jersey And Other Offshore Jurisdictions" (23 July 2008)

112. Westin A Privacy and freedom (Fifth ed.). New York، U.S.A.: Atheneum (1968)

113. Westin A. Privacy and Freedom، New York: Atheneum. (1967)

114. Westin، A. Privacy and freedom (Fifth ed.). New York، U.S.A.: Atheneum (1968)

115. Willard Marriott Library Japanese-Americans Internment Camps During World War II. 16 April (2007)

116. William J. Clinton & Albert Gore، Jr.، A Framework for Global Electronic Commerce، July 1، 1997

117. Williams، M. "Virtually Criminal: Crime، Deviance and Regulation Online"Routledge، London (2006)

118. Witten، Ian H.; Frank، Eibe; Hall، Mark A. Data

Mining: Practical Machine Learning Tools and Techniques (3 ed.). Elsevier 2011).

119. Yar، M. Cybercrime and Society، London: Sage. (2006)

2. Articles

1. Note، Keeping Secrets in Cyberspace:Estabishing Fourth Amendment Protection for Internet Communication، 110 HARV. L. REV. 1591 (1997).

2. Amitai "The Privacy Merchants: What is to be done?". The Journal of Constitutional Law (March 2012).

3. Andru E. Wall، Prying Eyes:The Legal Consequences of Reading Your Spouse's Electronic Mail، 30 FAM. L.Q. (2003)

4. Angela Choy، MarciaS.Smith and Jane Bortnick Griffith، Protecting privacy on the internet: a summary of legislative proposal، ”CRS Report for Congress، Congressional Reasearch Service، The liberary of Congress” (1997)

5. Ann Cavoukian، Ph.D.and Khaled El Emam، Ph.D ، Dispelling the Myths SurroundingDe-identification: Anonymization Remains a Strong Tool for Protecting Privacy، Information and Privacy Commissioner، Ontario، Canada (2011)

6. Annabelle. "Feminism، Democracy and the Right to Privacy." (Archove) Minerva - Journal of Philosophy

7. Arnold H. "Morals Legislation and the Establishment Clause". Alabama Law Review 55 (1) (2003).

8. Asscher، L، Hoogcarspel، S.A، Regulating Spam: A European Perspective after the Adoption of the E-Privacy Directive (T.M.C. Asser Press 2006)

9. Atchinson، Brian K.; Fox، Daniel M "The Politics Of The Health Insurance Portability And Accountability Act". Health Affairs (1997)

10. Bermann، S. Information Privacy، Official Reference for the Certified Information privacy Professional (CIPP)، Swire(2007

11. Blanchette، J.F.، & Johnson، D.G.. Data retentionandthe panoptic society: The social benefits of forgetfulness..The Information Society (2002)

12. Bloustein، Edward J Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser; N.Y. U Law review(1964)

13. Borking J. 'Privacy Protecting Measures in IT Environment Necessary'، Information Management، 10، (1998)،

14. Bracy، Jedidiah. Westin's Privacy Scholarship، Research Influenced a GenerationGR.trnd (2013)

15. Brendan Sasso ConsensusBuilds forRequiring Warrant forEmail(The Hill Searches،) (2013)

16. Bright، Peter "Doxed: how Sabu was outed by former Anons long before his arrest". ArsTechnica. (2012)

17. Burkert، H Institutions of Data Protection: An Attempt at a Functional Explanation of European National Data Protection Laws. Computer Law Journal، (1982)، 3 (2)

18. Bygrave L. Data Protection Law: "Approaching Its Rationale، Logic and Limits"Coma Press(2002)

19. Cavoukian Ann Who Knows: Safeguarding Your Privacy in A Networked WorldRandom House of Canada: (1995).

20. HarisseCastagnoli، Someone's Been Reading My E-Mail! Privacy Protection for Electronic Mail Users in the US and EC، 9 COMPUTER، L. & PRAC.، (1993).

21. Charlene Brownlee and Blaze D. Waleski Privacy Law،، Law Journal Press، New York، 2006، 2008

22. Charles Doyle Cybercrime: An Overview of the

Federal Computer Fraud and Abuse Statute and Related Federal Criminal Laws، Congressional Research Service، (2010)

23. Charles Doyle Privacy: An Overview of the Electronic Communications Privacy Act، Congressional Research Service، (2012)

24. Cooper، Marion B. Drinker Biddle &Reath LLP "January 1، 2013: New Fair Credit Reporting Act "FCRA" Forms Required by New Enforcement Agency". TNL Review. (2013)

25. Cooper، Marion B.; Drinker Biddle &Reath LLP "January 1، 2013: New Fair Credit Reporting Act "FCRA" Forms Required by New Enforcement Agency". TNL Review.، (2013)

26. Cormick، Michelle. "New Privacy Legislation." Beyond Numbers، ProQuest. (2003)

27. David Banisar The Right to Information and Privacy: Balancing Rights and Managing Conflicts، Global Campaign for Free Expression World Bank Institute Governance Working Paper.، (2011)

28. David Price New Study: The Size and Scope of Global Internet Piracy is on the Rise [VIDEO] of NetNames(2014)

29. Davis، Darren and Brian Silver. "Civil Liberties

vs. Security: Public Opinion in the Context of the Terrorist Attacks on America." American Journal of Political Science. Vol. 48. 1. (2004)

30. Deighton، J.A The Presentation of Self in the InformationAgeHarvardBusinessSchool Working Knowledge. (2006).

31. Dorothy J. Glancy "The Invention of the Right to Privacy"، Arizona Law Review، v.21، n.1

32. Doug Stanglin "School district accused of spying on kids via laptop webcams". USA Today. (2010)

33. Elsa F. Kramer، The Ethics of E-Mail، RES GESTAE، Jan. (1996)

34. Fenwick and G. Phillipson، "Breach of Confidence as a Privacy Remedy in the Human Rights Act Era" Modern Law Review 660 (2000)

35. France E. 'Using Design to Deliver Privacy'، in One World، One Privacy، Towards an Electronic Citizenship، 22nd International Conference on Privacy and Personal Data Protection، Venice، 2830-(September 2000)،

36. Frieden، Jonathan D.; Roche، Sean Patrick "E-Commerce: Legal Issues of the Online Retailer in Virginia"، Richmond Journal of Law and Technology (2006)

37. Geal RF Federal Trade Commission، Fair Information Practice Principles، (FIPs) review (2009)،

38. Greenleaf، Graham. "Global Data Privacy Laws: 89 Countries، and Accelerating". Social Science Electronic Publishing، Inc. Retrieved 16 February (2014)

39. Grimmelmann، James "Saving Facebook". Iowa Law Review (2009)..

40. Guadamuz A، 'Habeas Data: The Latin-American Response to Data Protection'، The Journal of Information، Law and Technology (JILT 2000) (2)

41. Fenwick H. and G. Phillipson، "Confidence and Privacy: A Re-Examination" Cambridge Law Journal 447.(1999)

42. Halder، D.، &Jaishankar، K Cyber crime and the Victimization of Women: Laws، Rights، and Regulations. Hershey، PA، USA: IGI Global.. (2011)،

43. Harold C. Relyea Privacy Protection: Mandating New Arrangements to Implement and Assess Federal Privacy Policy and Practice (CRS Report RS21851) (May 27، 2004)

44. Hollwitz، J. "The Development of a Structured

Ethical Integrity Interview for Pre-Employment Screening." The Journal of Business Communication (1997)

45. Hoofnagle، Chris Jay Identity Theft: Making the Known Unknowns Known". Harvard Journal of Law and Technology"، Vol. 21، (2007)

46. Hopwe، M. A Short Guide to the Freedom of Information ActandOther New Access Rights The Campaign for Freedom of Information، (2010)

47. Hugl، Ulrike "Reviewing Person's Value of Privacy of Online Social Networking، " Internet Research، (2011)،

48. Jacobson Amendments to the Constitution of Sweden"، Ministry of justice (2002)

49. Jain، A.K.; Bolle، R.; Pankanti، S.، eds. Biometrics: Personal Identification in Networked Society. Kluwer Academic Publications(1999).

50. Jain، Anil K.; Ross، Arun "Introduction to Biometrics". In Jain، AK; Flynn; Ross، A. Handbook of Biometrics. Springer (2008).

51. Jaishankar، K Cyber Criminology: Exploring Internet Crimes and Criminal behavior. Boca Raton، : CRC Press، Taylor and Francis Group. (2011)

52. Jarrett، H. Marshall; Bailie، Michael W. "Prosecution of Computer Crimes". Office of Legal Education Executive Office for United States Attorneys.، (2010)

53. Jason Angiulo and Grant Kleinwachter Privacy in a Transparent World Ethica Publishing، (2010)

54. Jensen، Carlos Privacy policies as decision-making tools: an evaluation of online privacy notices، Press Releases، (2004).

55. Jerry Berman&Deirdre Mulligan، Privacy in the Digital Age: Work in Progress، Nova Law Review، Volume 23، Number 2، The Internet and Law، (Winter 1999)

56. Joel Reidenberg information law and privacy، a U.S. Says(2014)

57. Johanna Granville، " Dot. Con: The Dangers of Cyber Crime and a Call for Proactive Solutions، " Australian Journal of Politics and History، vol. 49، no. 1 (2003)

58. John Villasenor، RecordingEverything Digital Storageas anEnablerof Authoritarian Governments، Brookings Institution

59. John H.F. Shattuck "Right of privacy" press view،

1966، P2.، see also Richard A. Posner، "The Right of Privacy، " 12 Georgia Law Review 393 (1977).

60. John M.K PII: Personal Identifiable Information p، US press release (1999)

61. John Woulds A Practical Guide to the Data، ProtectionAct، December 2004، Published by The Constitution Unit School of Public Policy، UCL، 29–30 Tavistock Square، London

62. Jonathan D. Frieden and Leigh M. Murray، The Admissibility of Electronic Evidence Under the Federal Rules of Evidence، XVII Rich. J.L. & Tech. (2011)

63. Kalman، Laura; Garrow، David Review: The Promise and Peril of Privacy". Reviews in American History (The JohnsHopkinsUniversity Press) (1994).

64. KamaalZaidi، Harmonizing U.S.-EU Online Privacy Law: Toward a U.S. Comprehensive Regime For the Protection of Personal Data، (2003).

65. Karen Kaplan ، In Giveaway of 10، 000 PCs، the Price is Users' Privacy Marketing: Recipients Must Agree to Let Pasadena Firm Monitor Where They Go on Internet and What They Buy، L.A. TIMES، (Feb. 8، 2009)

66. Kettle، Martin "World exclusive Tony Blair interview". The Guardian (London) (1 September 2010)

67. Kevien، M. "New draft European data protection regime". law group، (2003)

68. Kilman، Johnny and George Costello (Eds) "The Constitution of the United States of America: Analysis and Interpretation". GPO (2006).

69. Kirk Makin، " Ontario court paves way for victims of privacy intrusion to sue snoopers". Globe and Mai (201219-01-)

70. Kirsch، Michael S "Alternative Sanctions and the Federal Tax Law: Symbols، Shaming، and Social Norm Management as a Substitute for Effective Tax Policy". IowaLaw Review. (2004).

71. Krishnamurthy B، Wills CE On the Leakage of Personally Identifiable Information Via Online Social Networks،، US Press، (2009)

72. L. Castellani، 'The United Nations Electronic Communications Convention - Policy Goals and Potential Benefits'، Korean Journal of International Trade & Business Law 1 (2010)

73. Lanier and Saini Understanding Consumer Privacy: A Review and FutureDirections وAcademy of Marketing Science (2008)

74. Larose، R.، &Rifon، N. J. Promoting i-Safety: Effects of Privacy Warnings and Privacy Seals on Risk Assessment and Online Privacy Behavior. Journal Of Consumer Affairs، 41(1)، (2007).

75. Lee Bygrave Special Issue: Contemporary Issues in Internet Governance، Volume 22 Issue 1 Spring (2014).

76. Levi، Bozidar. UNIX Administration: A Comprehensive Sourcebook for Effective Systems and Network Management. CRC Press.2002

77. Levin، Richard C. Mark B. Myers. A Patent System for the 21st Century. Washington، D.C.: The National Academies Press (2004).

78. Marcia Coyle، Fretting over U.S. data collection: Critics see a lack of privacy protections، National Law Journal، (June 2، 2003)

79. Mark L. Goldstein and Lisa S. Vogel، Can You Read Your Employees' E-mail?" N.Y.L.J. (1997)

80. Marshall Jarrett Searching and Seizing Computers and ObtainingElectronic Evidence in CriminalInvestigations، Office of Legal Education Executive Office for United States Attorneys(2010)

81. Martin Hilbert and PriscilaLópez ، "The World's Technological Capacity to Store، Communicate،

and Compute Information"، especially Supporting online material، Science (journal)، (2011)

82. Mason، Alpheus Thomas Brandeis: A Free Man's Life، Viking Press، (1946)

83. McClennan، Jennifer P.Schick، Vadim "O، Privacy: Canada's Importance in the Development of the International Data Privacy Regime". Georgetown Journal of International Law 38 (2007).

84. Mediati، N. The Most Dangerous Places on the Web. PC World، 28(11)، (2010).

85. Mendelsohn، Stephen A.. "U.S. Department of Education Amends its FERPA Regulations to Allow for Certain Additional Student Disclosures". The National Law Review.(2012)

86. Metcalfe، Daniel J. "The Presidential Executive Order on the Freedom of Information Act" (PDF). 4th International Conferene of Information Commissioners. (23 May 2006)

87. Michael J. Ethics for the Information Age، Sun Press، (2009)

88. Michael J. Patrick، E-Mail Data Is a Ticking Time Bomb، NAT'L L.J.، Dec. 20، (1993)

89. Michael، J "Privacy and Human Rights: An

International and Comparative Study with Special Reference to Developments in Information Technology"، Dartmouth. (1994)

90. Moore، Adam D. Privacy Rights: Moral and Legal Foundations (PennsylvaniaStateUniversity Press، Aug.، 2010).

91. Morgan J. ، "Privacy، Confidence and Horizontal Effect: "Hello" Trouble Cambridge Law Journal 444، (2003)

92. Muench، David "Wisconsin Community Slogans: Their Use and Local Impacts"، December (1993)

93. Nancy Kim CLICKING AND CRINGING: MAKING SENSE OF CLICKWRAP، BROWSEWRAP AND SHRINKWRAP LICENSES، online article

94. Narayanan، A.; Shmatikov، V. "De-anonymizing Social Networks". 2009 30th IEEE Symposium on Security and Privacy (2009).

95. Narayanan، A.; Shmatikov، V. "Myths and fallacies of "personally identifiable information"". Communications of the ACM53 (6) (2010)

96. Nugter A.C.M. Transborder flow of personal data within the EC. Boston: Kluwer، (1990)

97. Patrick Wintour، "EU scraps timetable for ratifying constitution"، The Guardian press (London)، 2005

98. Paul A، J Mistakes Do Happen: A Look at Errors in Consumer Credit Reports". United States Public Interest Research Group. Archived from the original on (2006)

99. Paul E. Hash and Christina M. Ibrahim، E-Mail، Electronic Monitoring، and Employee Privacy، 37 SOUTH TEXAS LAW REVIEW 893 (1996).

100. Paul M. Schwartz & Daniel J. Solove، "The PII Problem: Privacy and a New Concept of Personally Identifiable Information"، 86 N.Y.U. L.REV. 1814 (2011)

101. Paul Ohm، University of ColoradoLawSchool، August 13، 2009، UCLA Law Review، Vol. 57، p. 1701، 2010، U of Colorado Law Legal Studies Research Paper No. 912-

102. Peter Jersey Data Protection In Jersey And Other Offshore Jurisdictions 23 July (2008) Article by Wendy Benjamin، mondaq. com، visited 2012 Sep

103. Peter P. Swire، Information Privacy، Official Reference for the Certified Information Privacy Professional (CIPP)، CIPP and Sol Bermann، CIPP، International Association of Privacy Professionals2007

104. Phillips، Melanie "From human rights to the EU، the tide's turning against the liberal thought police". Daily Mail (London). (4 July 2011)

105. Posner، R. A The economics of privacy. The American Economic Review، 71(2)، . (1981)

106. Puzis Rami، Yagil Dana، Elovici Yuval، and Braha Dan "Collaborative Attack on Internet Users' Anonymity."Internet Research (2012)

107. Singh R.and J. Strachan، "Privacy Postponed" European Human Rights Law Review[2003]

108. Rachel Cormier Anderson ، Enforcement of Contractual Terms in Clickwrap Agreements، Shidler J. L. Com. & Tech. 11 (Feb. 14، 2007)،

109. Randall Edwards Report: Privacy compliance is uneven، Federal Computer Week، (July 30، 2003)

110. Rechar، A، R Organization and it's privacy، Stock Books، 1987

111. Richard A. Posner "The Uncertain Protection of Privacy by the Supreme court"، the supreme court review the university of chigago press، Vol. 1979، (1979)

112. Richard A. Posner، The Economics of Privacy، The American Economic Review، Vol. 71، No.)2)،

Papers and Proceedings of the Ninety-Third Annual Meeting of the American Economic، Association (May، 1981)،

113. Rob Barrass، Lyndsay A. Wasser، "Seclusion intrusion: a common law tort for invasion of privacy". McMillan LLP.(2012)

114. Robert A. Hillman Online Boilerplate: Would MandatoryWebsite Disclosure of E-Standard Terms Backfireو‏MICH. L. REV. (2003)

115. Robert R. Schriver You Cheated، You Lied: the SafeHarbor Agreement and Its Enforcement By the Federal Trade Commission، 70 Fordham (2002)

116. Roger Clarke، The Supervisor's Dilemma:Is Reconciliation Possible between، the Candidate's Needs and the Supervisor's Integrity?، Slovenia، (June 2013)

117. Ron Condon،، Data Protection Act: UK information to avoid DPA fines، uk press، (2013)

118. Ronald. "Westin in Teaneck: Guiding a Magazine"، The New York Times، (1976).

119. Rumbaugh، Eric H.; Jason A. Kunschke; Michael Best & Friedrich LLP "Fair Credit Reporting Act Background Checks Remain a Hot Topic for Employers". The National Law Review. (2013)

120. Ryan، Falvey& Merchant Regulation of the Cloud in India،، Journal of Internet Law، Vol 15، No. 4 (October 2011).

121. Samuel Warren and Louis Brandeis، Law review article، Harvard Law Review.(1890)

122. Sawer، Patrick "Police use glove prints to catch criminals". Telegraph. co.uk. Retrieved 201313-12-2008) .20-08-)

123. Scott، Craig R "HIPAA Privacy Complaint Turns Into Federal Criminal Prosecution for First Time". Compliance Corner (University of Missouri Healthcare) (2012)

124. Shade، L. R، Reconsidering the right to privacy in Canada. Bulletin of Science، Technology & Society، (2008)

125. Shmatikov، V. " Myths and fallacies of "personally identifiable information، Communications of the ACM (2010).

126. Singletary، Michelle "Somewhat More Fair And Increasingly Accurate". The Washington Post (200311-12-)

127. Solove، Daniel J. Rotenberg، Marc، Schwartz، Paul M. Privacy، Information، and Technology، Aspen Publ. (2006)

128. Stephen F. Laribee& Stephen D. Hogan The Right to Privacy and Person Data: The EU Prods the U.S. and Controversy Continues، 9 Tulsa J. Comp. & Int'l L. (2002)

129. Susan W. Brenner، State Cybercrime Legislation in the United States of America: A Survey، 7 RICH. J.L. & TECH. 28 (Winter 2001)،

130. Tynan، Dan. "Real names، real problems: Pseudonymity under siege." ITWorld.، (2013)

131. Valcke. M، "T. Computers & Education". Elsevier Ltd.، (2012)

132. Vincent D. Blondel "Unique in the Crowd: The privacy bounds of human mobility". Nature srep (2013)

133. Virginia A Jones Requirements for Personal Information Protection، Part 1: U.S.Federal Law، CRM، FAI، (2008)

134. Warren and Brandeis "The Right To Privacy"، 4 Harvard Law Review 193 (1890)

135. Warren، S. D، and Brandeis، L. D “The right to privacy”، Harvard Law Review، (1890)

136. Weaver، A.C. "Biometric Authentication". Computer، 39 (2)، (2006).

137. William J. Clinton & Albert Gore، Jr “A Framework for Global Electronic Commerce”، (July 1، 1997)

138. William Prosser "Privacy"، California Law Review (Vol 48، No. 3، (1990)

139. Wilson J. "Health Insurance Portability and Accountability Act Privacy rule causes ongoing concerns among clinicians and researchers". Ann Intern Med (2006)

140. Wolf M، Bennett C. "Local perspective of the impact of the HIPAA privacy rule on research". Cancer، (2006)

141. Yael Onn، et al.، Privacy in the Digital Environment، HaifaCenter of Law & Technology، (2005)

142. YohkoOrito and Kiyoshi Murata "Privacy Protection in Japan: Cultural Influence on the Universal Value"، (2006)

143. ، Data Protection Act - non-compliance widespread، Bruce Ackland

144. Michael Cobb، Contributor، The 'appropriate' way to comply with Data Protection Act 1998، PoulWettnd، 2011.

3. Reports

1. "African Commission Criticizes Swaziland's Human Rights Record". Freedom House. 25، (2013)

2. "Did LulzSec، Trick Police Into Arresting the Wrong Guy? - Technology". The Atlantic Wire. (2011)

3. "Every expense spared"، The Economist، 19 December (2006)، Number 8532

4. "Lord Williams of Mostyn Memorial Lecture".، L.Williams، ukorg publications، 20011

5. "Protection of personal data - Justice". Ec.europa.eu. 201118-01-.

6. "The Universal Declaration of Human Rights: 1948–2008". United Nations

7. American Bar Association Task Force on the Federalization of Criminal Law، Report: Report on the Federalization of Criminal Law، 1998 A.B.A. SEC. CRIM. JUST. REP. 2

8. Annual Report on the Administration of the Privacy Act 20112012-

9. Article Jones Day، The legacy of ProCD v. Zeidenberg، Software License Jurisprudence، (2004)

10. Bergstein، Brian "Research explores data mining، privacy". USA Today Press (2006 P 67)

11. Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization By Michael Kassner in IT Security، September 14، (2009)

12. CIPSEA Report on confidentiality and data sharing from the U.S. Energy Information Administration retrieved from www.eia.gov (2013)

13. Consumer Privacy act report "Office of Justice Programs (OJP)، U.S. Department of Justice (DOJ)". Retrieved 2013

14. Data Protection، Where does processing occur?، "International Business Trade and Taxation" (March 2014)

15. Donalnd M، U.S.-SwissSafeHarbor Framework

16. ELEMENTARY DATA PROCESSING، Dr. Ikhu-Omoregbe N. A.&Afolorunso، A. A.، National Open University of Nigeria، Lagos. (2012)

17. Encryption:Impact on Law Enforcement،، "seal omitted FacilityQuantico، Virginia"، (1998)

18. Explanatory Report on the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Dat، Council of Europe، Startsbourg (1981)

19. Federalist Papers، #84. "On opposition to a Bill of Rights.". The Founders' Constitution. University of Chicago Press. Retrieved February 28، 2013

20. Focusing public attention on emerging privacy and civil liberties issues، "Electronic Privacy and Information Center: Choicepoint" P.21. EPIC. Retrieved 201319-11-.

21. GPS: Global Positioning System

22. Guidelines on the Protection of Privacy and Transporter flows of Personal data، (1980)،

23. ICT report، THE WORLD IN 2010، The rise of 3G، ICT Figers and Facts، (2010)

24. International Privacy Index". Electronic PrivacyInformationCenter (EPIC). (2013).

25. ITU (International Telecommunication Union) is the United Nations specialized agency for information and communication technologies – ICTs.

26. Making and Enforcing Contracts، Online، Provided by the Association of Corporate Counsel، 1025 Connecticut Avenue، NW، Suite 200، Washington، DC 20036 USA (September 2012)

27. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980)

28. Office of Justice Programs (OJP)، U.S. Department of Justice (DOJ)". Retrieved 2013

29. Privacy Commissioner's Report of Findings، "Law School Admission Council Investigation " May 29، (2006)

30. privacy" in Trischa Mann (ed.)، Australian Law Dictionary، Oxford Reference Online، Oxford University Press، accessed (29 August 2011)

31. ReportThe Guide to Data Protection، How much do Ineed to know about data protection?، ICO 2006

32. Report، THE PRIVACY ACT AND PERSONALLY IDENTIFIABLE INFORMATION U.S. Department of State Foreign Affairs Manual Volume 5 Information Management

33. Report، Review of the Implementation of the Human Rights Act، Department of constitutional Affaires، justice rights and democracy 2006

34. Report of the Secretary's Advisory Committeeon Automated Personal Data Systems U.S. Department of Health، Education & Welfare OHEW Publication NO. (OS) July (1973)

35. Report Privacy Protection Study Commission، Personal Privacy in an Information Society Congress press(July 1977)

36. Report Responding to gambling related crimes، report to Government department of tresuary and financeUSAOctober 2011

37. Report US Secretary's Advisory Committee on Automated Personal Data Systems، Records، Computers and the Rights of Citizens، Chapter IV: Recommended Safeguards for Administrative Personal Data Systems (1973).

38. Statewatch، US changes the privacy rules to exemption access to personal datacong.press2007

39. The Art of Forgetting in the Age of Ubiquitous Computing Faculty Research Working Papers Series:JohnF.KennedySchool of Government – HarvardUniversity. (2007)

40. The Center for Democracy and Technology's Snoop Demonstration at http://snoop.cdt.org/ for an example of the information that can be easily captured by sites on the World Wide Web.

41. The data protection (processing of sensitive personal data) order 2000، Made 17th February 2000

42. Coming into force - - 1st March 2000، united kingdom

43. the Electronic Privacy Information Centre 1998 – 2000

44. The European Union Data Privacy Directive، Berkeley Tech. (2000)

45. The Online Personal Privacy Act 2002، Sen. Ernest، reports، Office of Sen. Hollings، (2002)

46. The Organization for Economic Co-Operation and Development، “Guidelines on the Protection of Privacy and Transborder Flows of Personal Data”، available at http://www.oecd.org/document/18،0/2340، en_2649_34255_1815186_1_1_1_1، 00.html (last modified January 5، 1999)

47. The President’s Annual Report on the Agencies’ Implementation of the Privacy Act of 1974، ” CY 19821983-، at 118 (Dec. 4، 1985)

48. The rights of individuals (Principle 6)، ICO.gov.uk، accessed 14 April 2013

49. Transplanting Human Rights Norms: The Case of the United Kingdom's Human Rights Act". Human Rights Quarterly (2013).

50. What an IP Address Can Reveal About You، a report prepared by the Technology Analysis Branch of the Office of the Privacy Commissioner of Canada، (May 2013)

51. Invasion of privacy: Penalties and remedies: Review of the law of privacy: Stage 3" (2009) (Issues paper 14)، New Zealand Law Commission

52. U.S. Department of Justice، "Office of Privacy and Civil Liberties"، Overview of the Privacy Act of 1974

53. JudiciaryChairmanRobertGoodlatteto"lookatmodernizingthedecades`oldElectronicCommunicationsPrivacyAct(ECPA)$ to$ reflect$ our$ current$ digitaleconomy"). supra note، 2013

54. Independent Review of the impact of the Freedom of Information Act: A REPORT PREPARED FOR THE DEPARTMENT FOR CONSTITUTIONAL AFFAIRS"، Frontier Economics Ltd، October 2006. Retrieved on 201228-05-

4. Websites

1. Invasion of Privacy Law & Legal Definition، USLegalforms.com، retrieved October، 17، 2013. See also Solove، Daniel J.، Marc Rotenberg، and Paul M. Schwartz (2006)، Privacy، Information، and Technology، Aspen Publishers

2. http://www.magnac.com

3. http://www.esdc.gc.ca/eng/transparency/ati/reports/annual_privacy/2011_2012/index.shtml

4. http://www.ssa.gov/foia/html/disclosure_law.htm retrived at 22-12-2013

5. http://www.businessdictionary.com/definition/privacyretrived 7-6-2014

6. www.oecd.org

7. The law text available at http://itlaw.wikia.com/wiki/Category: Legislation-Sweden-Privacyretrived72014-6-

8. http://www.bundestag.de/aktuell/archiv/2007/innen_kw10/index.html>

9. https://www.privacyinternational.org/reports/germany/i-legal-framework

10. https://coeia.ksu.edu.sa Accessed202013/3/

11. http://icsa.cs.up.ac.za/issa/2004/Proceedings/Full/078.pdf. Accessed 16 July(2012)

12. "Asturalia Privacy Act 1988". Retrieved 14 -102013-.

13. http://web.archive.org/web/20100813133308/http://www.priv.gc.ca/keyIssues/ki-qc/mc-ki-pipeda_e.cfmretrived232012-7-

14. https://www.priv.gc.ca/leg_c/interpretations_02_e.aspp.100

15. http://www.brennancenter.org/resources/downloads/nation_security_brennan.pdf.

16. https://www.priv.gc.ca/leg_c/interpretations_02_e.asp

17. http://en.wikipedia.org/wiki/Magna_Cartap.34

18. http://en.wikipedia.org/wiki/Twelve_Articles

19. http://en.wikipedia.org/wiki/Declaration_of_the_Rights_of_Man_and_of_the_Citizen

20. : http://en.wikipedia.org/wiki/United_States_Bill_of_Rights

21. http://conventions.coe.int/treaty/fr/Treaties/Html/005.htm

22. http://www.oecd/document

23. http://ec.europa.eu/justice/policies/privacy/modelcontracts/index_en.htm

24. https://www.priv.gc.ca/leg_c/interpretations_02_e.asp

25. http://elj.warwick.ac.uk/jilt/002-/guadamuz.html

26. http://www.oecd.org/document/180،2340/، en_2649_34255_1815186_1_1_1_1،00.htm

27. www.un.org/law/avl

28. .publicationsduquebec.gouv.qc.ca. 2012

29. http://www.abanet.org/crimjust/fedreport.html.

30. http://laws-lois.justice.gc.ca

31. http://www.cnil.fr/

32. http://ec.europa.eu/justice/data-protection/index_en.htm

33. http://ico.org.uk/for_organisations/data_protection 22013/5/ P.10

34. http://www.edoeb.admin.ch/org/00129/index.html?lang=en

35. http://itlaw.wikia.com/wiki

36. http://www.f-law.net/law/threads

37. http://www.privcom.gc.ca/speech/archive/02_05_a_000128_e.asp

38. http://foia.state.gov/Learn/PrivacyAct.aspx retrived 122013-6-

39. http://www.mmmlaw.com/media-room/publications/articles/privacy-data-mining-on-the-internet

40. http://thomas.loc.gov/cgi-bin/query/z?c105:S.376retrived 122013/5/

41. http://www.techlawjournal.com/cong107/privacy/hollings/20020418summary.asp

42. https://www.govtrack.us/congress/bills/112/s1732/text

43. http://ico.org.uk/Global/~/media/documents/library/Data_Protection/Practical_application/THE_GUIDE_TO_DATA_PROTECTION.ashx

44. http://www.swissinfo.ch/ara/detail/content.html

45. https://www.un.org/News/Press/docs/2013/gashc4094.doc.ht

46. http://www.gartner.com/technology/supply-chain-professionals.jsp

47. http://www.research.att.com/projects/privacystudy/

48. http://www.wired.com/news/print_version/politics/story/16749.html?wnpg=all

49. https://www.law.stanford.edu/sites/default/files/event/266730/media/slspublic/Kim_clicking_and_cringing.

50. http://www.truste.org

51. BBB Online http://www.bbbonline.org/privacy/fr_bd_ix.html

52. Online Privacy Alliancehttp://www.privacyalliance.org/

53. http://www.adaweya.net/showthread.php?t=39298

5. Theses

1. de Silva، Richard "Government vs. Commerce: The Cyber Security Industry and You (Part One)". Defence IQ(11 Oct 2011). 2014.

2. Graham، Mark "Warped Geographies of Development: The Internet and Theories of Economic Development" (PDF). Geography Compass(2008)

3. Marh John Trane "Comments of Latanya Sweeney، Ph.D. on "Standards of Privacy of Individually Identifiable Health Information"". CarnegieMellonUniversity

4. Mark E L.Engaging Privacy and Information Technology in a Digital Age National Research Council of the National Academies، (2007).

5. Prof. Dr. Ulrich Sieber، “Legal Aspects of Computer-Related Crime in the Information Society

6. “(COMCRIME Study) (Jan. 1، 1998)

6. Acts

1. "Directive 9546//EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such dataavailble at wwww.eumpcouncil.org

2. Advisory Guidelines On Key Concepts In The Personal Data، Protection Act، Issued By The Personal Data Protection Commission، (24 September 2013)

3. Directive 200624//EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 200258//EC Magna Carta

4. Section 2(1) of the "Personal Information Protection and Electronic Documents Act " (2000، c. 5)

5. United States Bill of Rights

6. "Aboriginal Protection Act 1869 (Vic)". Documenting Democracy. National Archives of Australia. 2007

7. European Commission - Protection of personal data

8. Swiss Federal Data Protection Act (DPA)

9. Electronic Communications Privacy Act of 1986 (ECPA)،

10. Encrypt Communications Privacy Act of 1997

11. The Privacy Act Modernization for the Information Age Act of 2011

12. Data Protection Act 1998، Part IV (Exemptions)، Section 36، "Office of Public Sector Information"، accessed 6 September (2007)

13. The Data Protection Act 1998 (DPA) is a United KingdomAct of Parliament which defines UK law on the processing of data on identifiable living people

14. Directive 9546//EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such dataOfficial Journal L 281، 231995/11/ P. 0031

15. Council of Europe، Project on Cybercrime. (032007/13/). Cybercrime legislation –country profile. United States of America. URL: http:// www. cyberlawdb. com/ docs/ usa/ usa. pdf. retrived 012013/17/

الفهرس



www.ascpublishing.com



